Measures of Effectiveness for the Information-Age Navy

The Effects of Network-Centric Operations on Combat Outcomes

Walter Perry • Robert W. Button • Jerome Bracken • Thomas Sullivan • Jonathan Mitchell

RAND

Measures of Effectiveness for the Information-Age Navy

The Effects of Network-Centric Operations on Combat Outcomes

Walter Perry
Robert W. Button
Jerome Bracken
Thomas Sullivan
Jonathan Mitchell

Prepared for the

United States Navy

Approved for public release; distribution unlimited

RAND
NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was sponsored by the United States Navy. The research was conducted in RAND's National Defense Research Institute, a federally funded research and development center supported by the Office of the Secretary of Defense, the Joint Staff, the unified commands, and the defense agencies under Contract DASW01-01-C-0004.

Library of Congress Cataloging-in-Publication Data

Measures of effectiveness for the information-age Navy : the effects of network-centric operations on combat operations / Walter Perry ... [et al.].
p. cm.
"MR-1449."
Includes bibliographical references.
ISBN 0-8330-3139-2
1. Command and control systems—United States—Evaluation. 2. United States. Navy—Data processing—Evaluation. 3. Naval battles—United States. I. Perry, Walt L.

VB212 .M43 2001
359.3'3041—dc21

2002024917

RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND® is a registered trademark. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

U.S. Navy photos used in illustration. No expressed or implied endorsement.
Cover design by Stephen Bloodsworth

Published 2002 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 102, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information,
contact Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

PREFACE

The Navy is formulating new visions, strategies, and concepts that capitalize on emerging information-age technologies to provide its warfighters with significantly improved capabilities to meet the national security challenges of the twenty-first century. A key tenet of Joint Vision 2020 is that information superiority will enable such new operational concepts as network-centric warfare that promise decisive advantages over future adversaries. The evaluation of information superiority concepts will require new models and measures that capture the effects of improved command and control on information superiority and, more important, on combat outcomes. This report will be of interest to those involved with improving Navy targeting, assessment, and information technology.

RAND has been asked to develop measures of effectiveness (MOEs) that reflect the effects of changing command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) processes on combat outcomes in a network-centric environment. This report presents analyses of two combat vignettes—one involving defense against a combined ballistic missile and cruise missile threat and the other involving detection and destruction of time-critical targets. Mathematical relationships linking network-centric operations, C4ISR, combat operations, and combat outcomes in a common framework have been developed. The process introduces C4ISR MOEs, demonstrates means of evaluating them, and shows how they can be linked to combat outcomes.

This research was conducted for the Assistant for Strategic Planning (N6C), Department of the Navy, Office of the Chief of Naval Operations, within the Acquisition and Technology Policy Center of RAND's National Defense Research Institute (NDRI). NDRI is a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the unified commands, and the defense agencies.

CONTENTS

Chapter Three

Chapter Four

FIGURES

TABLES

SUMMARY

The primary objective of this work is to create a framework for developing measures and metrics that adequately assess the impact of varying command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems and procedures on combat outcomes. In the process, sample measures and metrics are suggested to achieve this goal.

Although measures are simply *bases* or *standards* of comparison and can therefore be described qualitatively, metrics must be mathematical expressions that allow us to evaluate not only the relative effect of alternative C4ISR systems on combat outcomes but also the degree to which one is better or worse than another. This argues for strict mathematical formulations that produce accurate results. It is important to note, however, that the process reported in this document is deductive—i.e., none of the equations presented in the text was based on experimental or operational data. Verification, validation, and calibration remains a task for future work.

The framework and the measures and metrics developed are demonstrated using a spreadsheet model based on techniques including graph and complexity theory, reliability theory, search theory, information entropy theory, and queuing theory. The objective is to demonstrate a proof-of-concept tool that can quickly generate several alternatives based on varying operating procedures, network connectivity, and C4ISR systems.

BACKGROUND

Traditional measures of effectiveness (MOEs) usually ignore the effects of information and decisionmaking on combat outcomes. In the past, C4ISR operations have been analyzed separately using measures of performance (MOPs). The effects of changes in C4ISR operations on combat outcomes have been inferred rather than directly assessed, and therefore the quantifiable link between variations in C4ISR capabilities and combat outcomes has been relatively difficult to assess.

Add to this the assertion that a richly connected network of C4ISR facilities and weapon systems will improve decisionmaking and therefore favorably impact combat operations and the assessment problem becomes even more complicated. This latter idea is embodied in the concept of network-centric warfare (NCW).

Network-Centric Warfare

Network-centric warfare is generally thought to be *the linking of platforms into one, shared awareness network in order to obtain information superiority, get inside the opponent's decision cycle, and end conflict quickly.* In contrast to network-centric operations or warfare, traditional warfare is considered to be *platform-centric.* The difference between the two is that in platform-centric warfare, one must mass force to mass combat effectiveness because each weapon system acts independently, whereas in network-centric warfare effects are massed, rather than force. That is, weapon system employment is "optimized" to improve aggregate performance, possibly at the expense of individual unit performance.

The Framework

The framework adopted in this report uses graph theory to assess the value or cost of connectivity and information theory to assess the value of collaboration in the context of simple operational models.

Graph theory can be used to represent the flow of data and information in naval warfare. It can be used to differentiate full participants in decisionmaking from outside monitoring. It can also be used to represent the complexity of data or information flow in decision processes. Once data and information pathways have been established, the decisions to be supported are determined and decision rules are developed.

Information theory is used to assess the "amount" of knowledge available in a command and control system. To do this, we apply the concepts embodied in information entropy or Shannon entropy. Where uncertainty exists, information entropy can be assessed—provided the uncertainty can be expressed as a probability. In general, entropy measures the amount of information available in the distribution. We use this to make the intellectual leap to measuring the knowledge level about the uncertain random variable. The additional information made available by collaboration increases the reliability of situation assessments, so reliability theory is a useful tool for studying collaboration. In the Time-Critical Target (TCT) vignette, we demonstrate how a priori knowledge (in this case of target behavior) can be combined with knowledge gained through collaboration. In the same vignette, we also demonstrate how knowledge improvements can be quantified in a way meaningful to operators.

Command and control alternatives, such as Cooperative Engagement Capability (CEC), are evaluated in this paper using simple sensor and weapon models to demonstrate the feasibility of analyzing the benefits of any improved information and the cost of possible information overload.

Analysis Implications for NCW

NCW is not just about networks. Networks are necessary but are not a sufficient ingredient to effective network-centric operations, and performance may or may not improve significantly with increases in network size. Instances may occur in which burdens of network complexity outweigh gains of increased opportunity to collaborate.

In addition, collaboration is generally, but not always, beneficial. Among the factors that affect the value of collaboration is the knowledge the decisionmaking team members possess about the critical element(s) of the operation and their level of experience in acting as a team. A team capable of highly effective collaboration is not apt to benefit appreciably from additional members—regardless of the new members' knowledge.

THE SCENARIO

The conflict hypothesized involves a small island country facing a large hostile neighboring nation determined to annex the island. The fact that the primary attack routes are over water, along with the small island country's dependence on sea lines of communication (SLOCs) and air lines of communication (ALOCs), implies a significant naval component. Setting the conflict 10 years into the future provides time to implement emerging NCW concepts as well as some new Navy systems.

The island's strategic objective is to "hold on" against an anticipated massive enemy application of force early on. The enemy hopes that this will force an early capitulation. At a minimum, the island nation must hold out until the U.S. intervenes. Figure S.1 illustrates the situation as the island prepares to defend against an anticipated attack.

U.S. forces are positioned to assist the island improve its defensive posture against enemy missile attacks. Two carrier battle groups (CVBGs) will be positioned east of the island. Cruisers and destroyers will screen the carriers with additional cruisers assigned ballistic

RANDMR1449-S.1

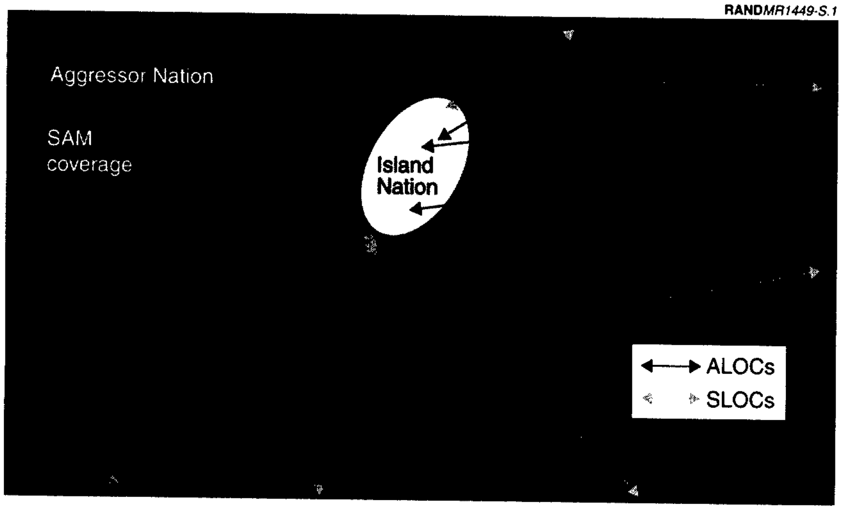


Figure S.1—Theater of Operations

missile defense duty off the island's two main ports. Nuclear-powered attack submarines (SSNs) will be assigned antisubmarine warfare responsibilities against enemy interdiction submarines.

CRUISE MISSILE AND BALLISTIC MISSILE DEFENSE

This first vignette examines the information aspects of ship defense against antiship cruise missiles (ASCM) while those ships conduct theater ballistic missile defense (TBMD). Once launched, cruise missiles and ballistic missiles enter an initial engagement queue. If no interceptor missile defeats the incoming attack missiles, one of two things will occur: ASCM leakers will join a second queue to be "serviced" by the Close-In Weapon System (CIWS) on board the cruisers or ballistic missile damage to land targets will be assessed.

Two pairs of Aegis cruisers are assigned to cover an area of operations to defend against enemy cruise and ballistic missile attack. Given their role in defending friendly territory, the cruisers themselves are also likely to be targets, and therefore they are prepared to defend against such an attack.

Measures of Performance and Force Effectiveness

The Aegis cruisers have two (competing) missions: prevent enemy ballistic missiles from destroying key allied infrastructure targets and defend against cruise missile attacks. For both missions, the obvious measure of success is survivability—that is, *the fraction of the critical infrastructure targets that survive the attack and the "fraction" of the cruisers that survive the attack.*

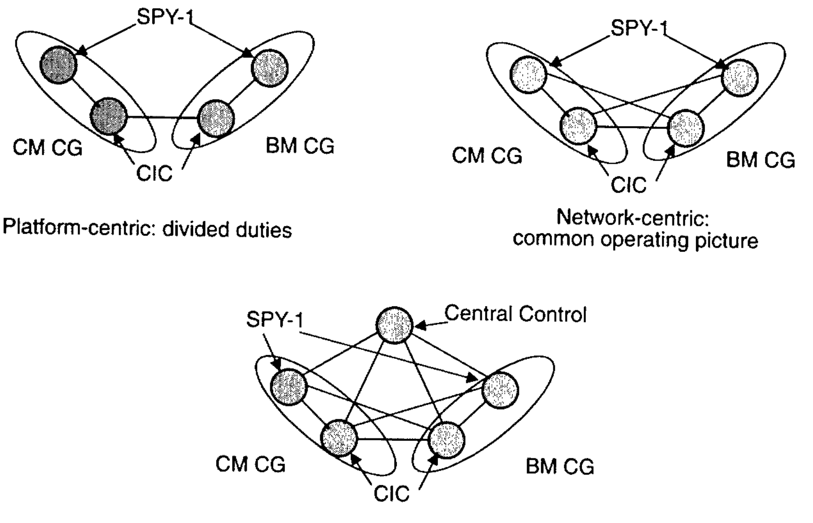
What is not known is the attack distribution for ballistic missiles and cruise missiles—i.e., how the enemy will schedule the attack to ensure that the friendly infrastructure targets are destroyed while at the same time minimizing interference from the defending cruisers. For purposes of this analysis, all other factors are known. The MOP therefore is *the degree to which the friendly commander "knows" the enemy's attack distribution.* Knowing the attack distribution contributes directly to the allocation of interceptors and therefore to the effective defense of both the cruisers and the friendly infrastructure targets.

Alternatives

Aegis cruiser radars cannot operate simultaneously against cruise and ballistic missiles; defensive responsibilities must be split between the two ships. We examine three alternatives: operations with divided duties, independent operations using a shared common operating picture (COP), and coordinated operations using a cooperative engagement capability. Figure S.2 illustrates each.

Platform-Centric Operations, Divided Duties: The two cruisers operate almost autonomously. That is, although they remain in contact with each other, no mechanism on board either ship automatically shares information on the arriving threat and/or firing solutions and no central authority directs the defensive response. Both ships employ a first-in-first-out (FIFO) queue discipline policy for engaging incoming missiles. For cruise missiles, this makes self-preservation

RANDMR1449-S.2



Platform-centric: divided duties

Network-centric:
common operating picture

Network-centric: cooperative engagement

NOTE: The Aegis cruisers operate in pairs with one directing its SPY-1 radar to detect and track ballistic missiles, while the other directs its SPY-1 radar to detect and track ASCMs.

Figure S.2—Alternative Operating Procedures

collective. This means the ship designated to intercept cruise missiles does not give itself priority against attack.

Network-Centric Operations, Shared COP: In the shared COP mode, both ships can see incoming ballistic missiles and cruise missiles. An understanding exists between the two ships concerning the nature of the attack. Connectivity has been extended so that missile threat trajectory and arrival time information are shared electronically, and in this sense the two ships can collaborate. Although sensor information is shared, the two ships continue to operate independently. Both ships have cruise missile and ballistic missile defense responsibilities. As a result, poor "queue discipline" is likely because both ships may engage the same missile or fail to engage a missile that might have been engaged with better coordination.

Network-Centric Operations, Cooperative Engagement: This is the most compelling option and therefore is analyzed most fully. Both ships have access to complete defense solutions, and allocation of ships to targets is controlled centrally by one of the two ships engaged in the operation. We depict a separate node for this additional function for the controlling commander. Not only connectivity is required in this case, but also automated systems to assess the relevant factors that go into making the best decision. Both ships have cruise missile and ballistic missile defense responsibilities, as in the previous case.

Decisions

The decisions center on the allocation policy that best protects both cruisers and the critical infrastructure targets. Remaining inventories of SM-2 Standard missiles on board each ship are critical to the decision process. The consumption rate for these missiles depends on the length of the time period, the firing rate, the shooting policy, and the number of ships engaging each enemy missile. Dedicated anti–cruise missile (ACM) or anti–ballistic missile (ABM) ships may risk emptying their defensive magazines before the attack has concluded. To prevent this, the two ships could then reverse roles.

Platform-Centric, Divided Duties: Only the role-switching decision is modeled for this case. The decision to switch or not is made at the beginning of each period. The need to switch roles is based on remaining inventories of Standard missiles on either of the defending cruisers.

Network-Centric, Shared COP: Both ships act independently—but with shared information. Each ship engages the targets it feels it can best intercept. The decision to engage an enemy missile is based primarily on the relative location of the ship and the enemy missile. Consideration is also given to remaining inventories of missiles and the anticipated attack arrival rate for the next period.

Network-Centric, Cooperative Engagement: The decision to be made is which ship(s) should attempt to intercept each incoming cruise missile and how many missiles can each "safely" engage in each period. The difference between this decision and the shared COP case is that, in this instance, a central control authority makes the decision based on shared information from both ships. The assignment of ship(s) to conduct the defense against cruise missile attack is determined using a set of decision rules based on allocating ships to missiles to prolong the survivability of the cruisers while maintaining inventories of ACMs and ABMs as long as possible.

Mathematical Representations

Network complexity and collaboration are combined to provide an estimate of the number of cruise and ballistic missiles expected to arrive in the next and subsequent periods. These estimates are then used in the allocation decision rules. The estimates are as follows:

$$\hat{\lambda}_c = (1 - K_{cC_v}(\lambda))\frac{n_c}{T} + K_{cC_v}(\lambda)\lambda_c$$

$$\hat{\lambda}_b = (1 - K_{cC_v}(\lambda))\frac{n_b}{T} + K_{cC_v}(\lambda)\lambda_b$$

The terms $\hat{\lambda}_c$ and $\hat{\lambda}_b$ are the current estimates of the arrival rates of attacking cruise and ballistic missiles respectively. $K_{cC_v}(\lambda)$ represents the knowledge about the attack distribution informed by the complexity of the network and the collaboration that has taken place. The subscript v refers to the case being examined (v = 1—platform-centric, v = 2—COP, and v = 3—cooperative engagement). λ_c and λ_b are the true attack distributions and n_c and n_b are the attack sizes for cruise and ballistic missiles to be launched over a total of T minutes. The knowledge function is bounded between 0 and 1 with $K_{cC_v}(\lambda) = 1$ representing perfect knowledge. When this occurs, $\hat{\lambda}_{ci} = \lambda_{ci}$ and $\hat{\lambda}_{bi} = \lambda_{bi}$ and when knowledge is poor ($K_{cC_v}(\lambda) = 0$) we have that $\hat{\lambda}_{ci} = n_c/T$ and $\hat{\lambda}_{bi} = n_b/T$. This last case means our estimate is that the missiles are uniformly distributed over the attack horizon, T. These equations are the MOP. The effectiveness measures (survivability of cruisers and infrastructure) are assessed as a result of the decisions taken based on these measures.

A TIME-CRITICAL TARGET

The second vignette focuses on the problem of locating and destroying an enemy submarine Type 877 Kilo in a short period of time. It is known in advance that the Kilo will leave port to replace another enemy submarine killed by a U.S. SSN, and a plan is devised to kill it before it can threaten the SLOCs. Figure S.3 depicts the situation on D+10, the day the enemy submarine leaves port en route to a position north of the friendly island to menace shipping along the SLOCs. On D+6, a *Virginia*-class SSN begins a previously planned Intelli-

RANDMR1449-S.3

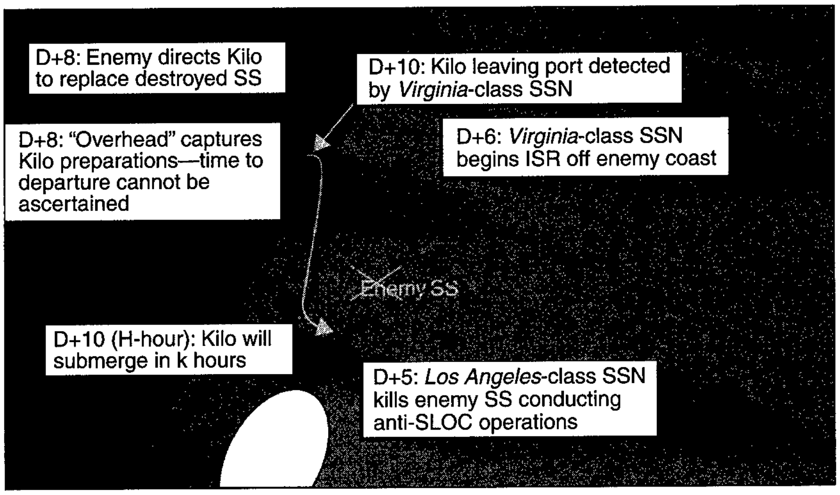

D+8: Enemy directs Kilo to replace destroyed SS
D+10: Kilo leaving port detected by *Virginia*-class SSN
D+8: "Overhead" captures Kilo preparations—time to departure cannot be ascertained
D+6: *Virginia*-class SSN begins ISR off enemy coast
Enemy SS
D+10 (H-hour): Kilo will submerge in k hours
D+5: *Los Angeles*-class SSN kills enemy SS conducting anti-SLOC operations

Figure S.3—Situation at D+10

gence, Surveillance, and Reconnaissance (ISR) mission off the enemy's coast. On D+10, it detects the Kilo leaving port and is able to track it as it moves toward its final station. The objective is to kill the Kilo on the surface as it emerges from the port without revealing the ISR submarine or disrupting its mission. An F/A-18 fighter attack aircraft will be vectored to the Kilo and will kill it using a Standoff Land-Attack Missile–Extended Response (SLAM-ER) missile.

Measures of Performance and Force Effectiveness

The Joint Task Force Commander (JTFC) has determined that catching the Kilo on the surface and attacking it as early as possible can best accomplish his objective. The command and control MOP therefore is *Time on Target*—the time available to an attacking aircraft to conduct its attack measured as the time elapsed between its arriving on station and the Kilo submerging. The combat MOE is the *probability that the SLAM-ER destroys the Kilo.*

Platform-Centric Operations. In this configuration, the ISR SSN reports to the operational commander, who would then alert the two CVBGs in the area that a threat submarine has left port. An F/A-18 is placed in "Alert 5" status and flies out to attack the Kilo from one of the CVBGs. The ISR SSN continues to provide updates on the Kilo through his operational commander. Command and control is split between the SSN and air operations personnel on the carrier. The SSN may attack the submerging Kilo without notifying other units. On the other hand, air operations might determine that the threat level to the aircraft was becoming excessive and abort the mission.

Network-Centric Operations. In this case, the connectivity among the participants is richer. The ISR submarine has two-way communications (via Link 16) to the carriers and the deploying aircraft. The controlling carrier uses two-way communications with the F/A-18 to control its operation and to confirm threat status updates. The F/A-18 receives periodic target updates directly from the ISR submarine. The command and control architecture has the same divisions as the platform-centric operation architecture, but consequences of this division are considerably reduced. For example, the ISR submarine may still decide that the Kilo is about to submerge and that the aircraft cannot attack in time and attack the Kilo itself. However, with communications directly to the carrier, and to the aircraft, the aircraft can be turned back earlier. Similarly, if air operations determines that the threat to the F/A-18 is excessive and it is turned back, the ISR submarine can be alerted in its next communication cycle and therefore have more time to attack the Kilo itself.

Future Network-Centric Operations. The Navy's Unmanned Combat Aerial Vehicle (UCAV) concept is currently under consideration by the Office of Naval Research (ONR). UCAVs are designed to be launched from a variety of surface combatants and therefore eliminate the burden of keeping an F/A-18 (and a catapult) on alert status for days. After the ISR submarine detects the Kilo coming out of port it alerts all potential UCAV launch ships. The ships receiving the message negotiate to determine which can get a UCAV to the Kilo first. Such issues as who makes the final selection, who determines when sufficient collaboration has occurred, what prior designations have been made, what is the polling frequency, and who determines which combatants with UCAVs are candidates are command and control procedural questions that must be addressed and evaluated analytically. A UCAV is then launched and begins to fly out to the Kilo Area of Uncertainty (AOU). The ISR submarine takes over control of the UCAV, including weapon release. The command and control architecture for this case is unsettled. Several options are available and constitute the basis for conducting exploratory analysis to determine the effects of each on combat outcomes.

Mathematical Representations

As with the missile defense vignette, network complexity and collaboration combine to affect combat operations. In this case however, the decision to attack is based on an assessment about the time required to get an attack platform (UCAV or F/A-18) in position to launch a weapon. The expected latency expression is as follows:

$$L_{cC} = \frac{1}{1-g(C)} \sum_{i=1}^{\tau} \prod_{j=1}^{d_i} [(1-K_j(t))^{\omega_j}] \frac{\delta_i}{\lambda_i},$$

where L_{cC} is the expected time required to get the attack platform on station given the effects of collaboration and network complexity. Table S.1 describes the terms in this expression. This is the MOP.

Table S.1

Definition of Terms for TCT MOP

Term	Definition
$g(C)$	The complexity factor $(0 \le g(C) < 1)$. Measures the effects of "information overload."
τ	The number of entities (nodes) participating in the operation.
d_i	The indegree of node i, i.e., the number of connections that terminate at node i.
$K_j(t)$	The knowledge gained from node j $(0 \le K_j(t) \le 1)$.
ω_j	The importance of node j. $\omega_j = 1$ if node j is participating in the operations and $\omega_j = 0.5$ if it is not.
δ_j	If node i is connected to node j, $\delta_j = 1$ otherwise $\delta_j = 0$.
$1/\lambda_i$	The mean time to complete the task required at node i.

The effectiveness of the operation depends on the probability that the enemy submarine will be detected and successfully engaged. This in turn depends upon the amount of time, $T = S - L_{cC}$, available to search and attack, where S is the time the submarine will submerge. We assume that the SLAM-ER is sufficiently effective so that if it detects a target, the target is destroyed with certainty. The MOE therefore is based on the search equation:

$$P_d(T) = 1 - e^{-\gamma T},$$

where $P_d(T)$ is the probability the submarine will be detected in T minutes or less. The coefficient γ consists of the geometrical aspects of the problem, such as the AOU, the sensor's field of regard, and its sweep width. Also, it includes the information update frequency from the ISR SSN and knowledge gained from external sources.

EXPLORATORY DATA ANALYSIS (EDA)

Changes in MOEs that result from modifying the levels of input variables are best understood by using visualization techniques. By varying the input variables, we can better understand the structure of the data and the complex relationships between inputs and MOPs/MOEs. This is most easily achieved by using a single representative value for some subset of inputs—essentially treating them as fixed and assigning two of the input variables to the x- and y-axes. Exploration is then conducted by interactively changing the fixed input values to better understand the relationship between that variable, the input variables shown on the axes, and the resulting MOE. A complete EDA has three phases:

- **Phase I—an introductory visual exploration:** This allows all possible inputs to occur with equal probability.
- **Phase II—a focused analysis:** The goal is to restrict the exploration to ranges of input variables that are more likely to occur.
- **Phase III—a full-scale stochastic simulation:** The simulation does not use the expected value of known distributions, but rather randomly draws from them at each simulation replication.

The EDA tool developed for this study focuses on the first two phases, where important relationships are discovered and the expected impact of policy decisions can be made before undertaking the more costly task of simulation.

CONCLUSION

We conclude as we began by stressing the need for new measures and metrics that incorporate the effectiveness of C4ISR systems, procedures, and equipment and their effect on combat outcome. The assertion is generally made that a richly connected network of C4ISR facilities and weapon systems will improve decisionmaking and therefore favorably impact combat operations. This may be true, but as yet we have no systematic, universally accepted way to demonstrate the truth of this claim. This report has focused on the Navy's early attempts at codifying one approach. Clearly, much remains to be done before accepted practices can be established. The work presented here is just a beginning.

Networks and NCW

NCW is not just about networks. Networks are necessary but not sufficient to ensure effective network-centric operations. Much has been made of the relationship between the "size" of the network and its efficiency. The computer network analogy is often cited to illustrate that a more richly connected network *ipso facto* improves overall performance.

A somewhat opposite claim is that the larger the number of connections in an operational network, the more likely individual nodes will experience "information overload." Both arguments are compelling. However, it remains to be seen if either is true when applied to military operations.

In this work, we suggest a way to assess both the good and bad effects of complexity with no claim that our representations are accurate. However, complexity alone, as defined by the number of connections in a network, is clearly not enough to assess the effectiveness of network-centric operations. The *command and control procedures* implemented on the network and the quality and extent of *collaboration* also play an important role.

Collaboration is expected to improve a process by which a team of individuals work together to achieve a common goal. We have argued that collaboration is important because it can enhance the degree of shared awareness in a group focused on solving a specific problem or agreeing on a decision. Although we have assumed that collaboration is generally beneficial, we have also recognized that it is not *uniformly* beneficial.

Information Theory

Information theory is not just a subset of communications theory, as some suggest. Rather it contributes to several fields of human endeavor, but, most important, it applies to military operations. In this work, we rely on information theory to assess the "amount" of knowledge available in a command and control system. To do this, we apply the important concept of information entropy or Shannon entropy.

The quality of collaboration is clearly related to the knowledge the participants in the decision team about the uncertain environment in which they operate. It is natural therefore to resort to the knowledge function, which is derivative of information entropy, to assess the effectiveness of the collaboration between two decision team members.

Next Steps

We have stated repeatedly that this is but a small first step in the effort to establish measures and metrics to connect C4ISR and network-centric operations to outcomes of combat. As a next logical step, the following areas should be researched:

- Improve understanding of network complexity and better characterize its effects.
- Improve understanding of the effects of collaboration.
- Examine ways to represent the multidimensional effects of collaboration.
- Assess the effects of information quality on the effects of collaboration.

ACKNOWLEDGMENTS

The authors recognize the helpful suggestions made by CAPT Robert Tylecki, Director of N6C, concerning the appropriate vignettes to address relevant naval operations, and Howard Wiener of N6C for his helpful comments on the technical approach adopted in this research and his detailed review of this report. We also thank RAND colleague David Signori and Thomas Lucas at the Naval Postgraduate School for their excellent reviews of the draft version of the report. Several faculty members at the Naval Postgraduate School at Monterey, Calif., contributed useful comments during the early analytical phases. Prominent among these are Wayne Hughes, William Kemple, and Donald Gaver. We are grateful for their assistance. We also wish to thank RAND colleague RADM (ret) Frank Lacroix for his guidance in designing the vignettes presented in this work and for sharing with us his personal experience as a submarine commander. Finally, we thank Karen Echeverri for completing the myriad administrative tasks required to publish this report.

ACRONYMS AND TERMS

ABM	Anti–ballistic missile
ACM	Anti–cruise missile
ALOC	Air Line of Communication
AOU	Area of Uncertainty
ASCM	Antiship cruise missile
ASW	Antisubmarine warfare
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CEC	Cooperative Engagement Capability: a capability that combines data from all platforms in an operation and allows the combined data to produce a better shared COP
CG	Guided Missile Cruiser
CIC	Command Information Center
CIWS	Close-In Weapon System
CJTF	Commander, Joint Task Force
Collaboration	A process in which operational entities actively share information while working together toward a common goal
Complete graph	A fully connected directed or undirected graph
Complexity	Having several interrelated parts as in a network with several interrelated operational entities

COP	Common operating picture: a view of the battlespace shared by all friendly forces
CVBG	Carrier battle group
CVIC	Carrier Intelligence Center
Directed Graph	A graph for which the direction of the edges connecting two nodes is considered
EDA	Exploratory data analysis
Directed Edges	Of a directed graph: arcs depicting direction of information flow between nodes; also referred to as "directed connections"
EW	Electronic warfare
Exploratory Analysis	The analysis of a large set of outcomes produced by varying input parameter sets
FIFO	First-in-first-out queue discipline
GPS	Global Positioning System
Graph	A collection of nodes and connecting edges used to represent a network
Indegree of a Node	The number of edges that have that node as their terminal node
Information Entropy	A measure of the average amount of information in a probability distribution. Also referred to as Shannon Entropy
Information Superiority	The ability to collect, process, and disseminate information as needed; anticipate the changes in the enemy's information needs; and deny the enemy the ability to do the same
INS	Inertial Navigation System
IPB	Intelligence Preparation of the Battlespace
ISMWG	Information Superiority Metrics Working Group
ISR	Intelligence, Surveillance, and Reconnaissance
JTFC	Joint Task Force Commander
Kilo	NATO designation for a Russian Project 877 Diesel-Electric Submarine

Knowledge	Accumulated and processed information wherein conclusions are drawn from patterns. In this report measured as normalized information entropy. See mathematical glossary below
LACM	Land-Attack Cruise Missile
Leakers	In this context, enemy missiles that elude friendly defense systems.
Measures	Standards for comparison.
Metrics	Mathematical expressions that evaluate both the relative effect of alternatives and the degree to which one is better or worse than another.
MODLOC	Miscellaneous Operational Details Local Operations: fixed, geographically defined operating areas
MOE	Measure of Effectiveness
MOP	Measure of Performance
NCO	Network-Centric Operations
NCW	Network-Centric Warfare
ONR	Office of Naval Research
OOC	Out of Commission
Polling	Request from a central authority for information essential to selecting one of several candidates to execute a mission
ROF	Ring of Fire (network-centric approach to littoral warfare)
SAM	Surface-to-Air Missile
Saturation	A condition occurring when the number of attacking missiles overwhelms the friendly defenses
SLAM-ER	Standoff Land-Attack Missile–Extended Response
SLOC	Sea Line of Communication
SM	Standard missile
SS	Attack submarine
SSN	Nuclear-powered attack submarine

SSPH	Single-Shot Probability of Hit
SSPK	Single-Shot Probability of Kill
Task Force	The nodes in the network actively engaged in the operation
TBM	Theater (or Tactical) Ballistic Missile
TBMD	Theater Ballistic Missile Defense
TCT	Time-Critical Target
TEL	Transportable-Erector-Launcher
UCAV	Unmanned Combat Aerial Vehicle
V/STOL	Vertical/Short Takeoff and Landing

GLOSSARY OF MATHEMATICAL TERMS

This glossary records the more important mathematical terms used in the report. The chapter reference is included because the same term may have different meanings in each chapter it appears.

Term	Definition	Chapter Reference
$A^{(b)}$	Designation for Aegis cruiser directing its SPY-1 radar to detect and track ballistic missiles	3
$A^{(c)}$	Designation for Aegis cruiser directing its SPY-1 radar to detect and track cruise missiles	3
n_c, n_b	The total number of launched cruise missiles and ballistic missiles, respectively, that are scheduled to "arrive."	3
$T = \tau t$	T is the total CM/BM attack time (in minutes) and τ is the number of attack time periods of duration t	3
λ_{ci}, λ_{bi}	The average arrival rates per minute in time period i for cruise and ballistic missiles, respectively	3

$\hat{\lambda}_{ci}, \hat{\lambda}_{bi}$	The estimated average arrival rates per minute in time period *i* for cruise and ballistic missiles, respectively	3
$g = \lambda_c t,\ g = \lambda_b t$	The number of cruise and ballistic missiles, respectively, arriving in a time period	3
p_c	The single-shot probability that a Standard missile intercept from an Aegis cruiser kills an attacking cruise missile	3
P_K	The effective probability that a Standard missile interceptor will kill an attacking cruise missile	3
$P_L = 1 - P_K$	The probability that an attacking cruise missile will be a "leaker"	3
$L_i = P_L \lambda_{ci} t$	The expected number of leakers in time period *i*	3
E_f	The expected number of Standard missiles that must be fired at each attacking cruise missile	3
h	The number of attacking cruise missiles *detected* at a given time	3
$\mu = \dfrac{1}{\tau_1 + \tau_2 + \tau_3}$	The mean time required for each Aegis cruiser to engage an attacking missile: τ_1 is the mean time to prepare a launcher, τ_2 the mean time required to launch the intercept, and τ_3 the mean time to fly out to the target	3
$\delta = \tau_1 + \tau_2$	The time required to prepare a Standard missile launcher for the next launch	3

N_L	The number of attacking cruise missiles required to destroy an Aegis cruiser	3
$V_0(x), V_1(x)$,	The maximum or target variance and the minimum variance, respectively, for the fraction of remaining missiles arriving in the current time period	3 and Appendix A
$H(x)$	$H(x)=E[\ln(f(x))]=-\int_{-\infty}^{\infty}\ln[f(x)]\mathrm{f}(x)dx$ Information or Shannon entropy. See Acronyms list for definition	3
$K(\lambda)$	The degree to which the attacking missile arrival rate is known. Calculated as the normalized $H(\lambda)$.	3
δ_c, δ_b	The minimum number of ACMs and ABMs needed to assume the role of defense against CMs and BMs, respectively	3
$I_c^{(c)}$, $I_b^{(c)}$	The remaining inventories of ACMs and ABMs on board $A^{(c)}$	3
$I_c^{(b)}$, $I_b^{(b)}$	The remaining inventories of ACMs and ABMs on board $A^{(b)}$	3
E_f	The number of Standard missiles required to destroy an enemy missile ($f = c$ implies ACM and $f = b$ implies ABM)	3
F_f	Estimate of the future attack ($f = c$ implies CM attack and $f = b$ implies BM attack)	3
$d_f^{(c)}$	The number of Standard missiles $A^{(c)}$ should launch against attacking enemy missiles of type f ($f = c$ implies CM attack and $f = b$ implies BM attack)	3

$d_f^{(b)}$	The number of Standard missiles $A^{(b)}$ should launch against attacking enemy missiles of type f ($f = c$ implies CM attack and $f = b$ implies BM attack)	3
$E_c(c), E_c(b),$ $E_c(b,c)$	The expected number of ACMs fired by $A^{(c)}$, $A^{(b)}$, or both	3
$E_b(c), E_b(b),$ $E_b(b,c)$	The expected number of ABMs fired by $A^{(c)}$, $A^{(b)}$, or both	3
$1/\lambda_i$	The mean time required to accomplish task i.	4
L, L_c, L_{cC}	The network latencies: base, with collaboration factored and with both collaboration and complexity factored	4

Chapter One

INTRODUCTION

Traditional measures of effectiveness (MOEs) usually ignore the effects of information and decisionmaking on combat outcomes. In the past, command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) operations have been analyzed separately using measures of performance (MOPs). Assessing the effects of improvements in C4ISR operations on combat outcomes has been inferred rather than directly assessed. For example, such physical improvements as greater bandwidth are generally thought to be beneficial to combat operations. The same is true for improved sensors and fusion algorithms and their salutary effects on the common operating picture (COP). Even the more recent discussions of network-centric warfare (NCW) or network-centric operations (NCO) (Cebrowski, 1998) and information superiority imply that their effects will be to improve combat operations by improving decisionmaking. However, the quantifiable link between these improvements in C4ISR and combat outcomes has been relatively difficult to assess. The problem has been widely recognized: for example, Alberts et al. (2001) state in their recent book:

> For many, Information Superiority and Network Centric Warfare remain abstract concepts, their applicability to military operations and organizations [are] unclear, and their value unproven. Others have seen the benefits but are unable to "connect the dots" between improved information . . . and outcomes in a [scientifically] rigorous . . . way.

NCW

NCW is generally thought to be *the linking of platforms into one, shared awareness network in order to obtain information superiority, get inside the opponent's decision cycle, and end conflict quickly.* In contrast to network-centric operations or warfare, traditional warfare is considered to be *platform-centric.* The difference between the two is that in platform-centric warfare, one must mass force to mass combat effectiveness because each weapon system acts independently, whereas in NCW effects are massed, rather than force. That is, the employment of weapon systems is *optimized* so that a target is serviced by the most effective system in the network.[1] Thus, it is hypothesized, the effects of massing force can be obtained with a much smaller force. The Navy and the C4ISR community are pursuing the application of this concept to warfare.

NCW is based on the concept of three network grids:

- **The information network grid:** The information grid provides the infrastructure to "receive, process, transport, store, and protect information for the Joint and combined services" (Stein, undated).
- **The sensor network grid:** The sensor grid is a need-based network that uses the sensors in the information grid pertinent to a given task. It is made up not only of such typical warfare sensors as radar but also of imbedded logistics sensors to track supply. The sensor grid is unique to each task.
- **The engagement-decision-shooter grid:** Sensor and warfighter elements of the network are tasked to attack in the engagement grid. This grid, like the sensor grid, is dynamic, using a unique blend of warfighters and sensors for each new task (Stein, undated).

The latter two grids are completely contained in the information network grid. Each grid is composed of nodes represented by individual sensors, weapons, or command platforms and is connected via networked data and communication. The sensor and engage-

[1] Actually, the word "optimized" is a bit strong. "Improved considerably" is closer to the truth.

ment grids are not necessarily separate. They often have overlapping components. For example, the sensor grid begins a track on a cruise missile and continues to track as the pertinent unit engages and a kill is made.

NCW flattens the command and control pyramid. Commanders communicate intent through the introduction of doctrine in the form of computer algorithms as well as communicating directly with individual units. NCW moves toward automated optimization of the positions of units in a group and engagement of enemy forces using new initiatives such as the Navy's Cooperative Engagement Capability[2] (CEC) and Ring of Fire.[3]

OBJECTIVES

The primary objective of this project is to create a framework for developing measures and metrics that adequately assess the impact of changed C4ISR systems and procedures on combat outcomes. In the process, sample measures and metrics are suggested that achieve this goal. These are presented with the idea of generating dialogue in the naval and C4ISR communities concerning the framework and the measures and metrics suggested. This is clearly overdue.

Although measures are simply *bases* or *standards* of comparison, and can therefore be described qualitatively, metrics must be mathematical expressions that allow us to evaluate, not only the relative effect of alternative C4ISR systems on combat outcomes, but also the degree to which one is better or worse than another. This argues for rigorous mathematical formulations that produce accurate results. It is important to note, however, that the process reported in this document is deductive—i.e., none of the equations presented in the text

[2] CEC is designed is to combine the raw sensor data from all platforms involved in an operation, regardless of age or type of sensors on individual platforms. It allows the combined data from these sources to produce a more complete, shared COP for tracking purposes. For additional information see "The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, 16/4, 1995.

[3] The Ring of Fire (ROF) concept is a network-centric approach to littoral warfare. It links land, sea, and air forces to produce calls for fire. Like the CEC, ROF networks sensor and weapon information for sea, shore, and command forces in the littoral to produce an extended and more accurate COP. See Mitchell, R., "Naval Fire Support: Ring of Fire," *US Naval Institute Proceedings*, 123/11:54, November 1997.

is based on experimental or operational data. Validation and calibration remain tasks for future work.

Naval warfare covers a wide range of disparate operations and, therefore, demands a variety of measures and metrics to assess the outcomes analytically. Consequently, it is important that an analysis of this kind encompass a variety of engagements to ensure the adequacy of the framework and the metrics developed. The objective then is to select a single major conflict and examine several vignettes within the scenario. The scenario selected was a notional future (2010) conflict involving the defense of threatened allied territory. Two vignettes were selected for examination:

- **Cruise and ballistic missile attack:** The first is a coordinated antiship cruise missile (ASCM) saturation strike against U.S. surface combatants and a ballistic missile attack against targets being defended by those surface combatants. An ASCM attack might prevent those ships from protecting against ballistic missiles by disabling a ship or saturating its command and control systems so that ballistic missiles can "leak" through.
- **Time-Critical Targets (TCTs):** The classic TCT vignette for analysis is operation against a Transportable-Erector-Launcher (TEL), such as an enemy Scud launcher. However, the vignette selected for analysis in this work is the search for and destruction of an enemy submarine leaving port en route to interdict friendly ports. The submarine must be destroyed before it submerges.

Finally, the framework and the measure and metrics developed are demonstrated using a spreadsheet model. The objective is to provide the analyst with a proof-of-concept tool that will quickly generate several alternatives based on varying operating procedures, network connectivity, and C4ISR systems. The relative value of the alternatives is assessed in terms of the contribution each makes to combat outcomes. The contribution may be defined differently for each vignette evaluated. Several hundred alternatives can be easily generated using the spreadsheet models, and therefore the use of *exploratory analysis* as an evaluation tool is required. "Exploratory analysis" refers to the use of many computational experiments to reason about complex and uncertain problems. Recently, exploratory approaches have been used for a variety of studies.[4]

ABOUT THIS REPORT

Chapter Two outlines the basic scenario developed to support this study. Several vignettes were developed from this scenario, and two were singled out for analysis. Chapter Three details the first of these: the defense of allied territory and the engaged fleet against ballistic missile and cruise missile attack. Chapter Four focuses on the second vignette: a TCT analysis problem involving the search for and destruction of a surfaced enemy submarine. Both Chapters Three and Four include the mathematical foundation for the metrics proposed to assess the relationships among NCW, improved command and control processes, and combat outcome. Chapter Five describes the spreadsheet model used to conduct exploratory analysis and Chapter Six concludes with some findings and suggestions for future work. Two glossaries are included to assist the reader with the text. These appear on pp. xxxi–xxxviii. The first describes acronyms and terms used in the text, and the second records the definitions of the several mathematical terms. Finally, an Information Entropy appendix is included.

[4] For a discussion of exploratory analysis and exploratory modeling, see Bankes (1993) and Davis, Bigelow, and McEver (2001).

Chapter Two

A FUTURE MARITIME CONFLICT

The conflict hypothesized involves a small island country facing a large hostile neighboring nation determined to annex the island. The fact that the primary attack routes are over water, along with the small island country's dependence on sea lines of communications (SLOCs) and air lines of communications (ALOCs), implies a significant naval component. Setting the conflict 10 years into the future provides time to implement emerging NCW concepts as well as some new Navy systems.

THE ENEMY'S PLAN

The scenario begins early in 2009, as the hostile nation prepares to attack the nearby island nation. By May 2010, planning is complete and the enemy is ready to initiate operations against the island. From the enemy's perspective, the most favorable outcome would be for the island to capitulate before the United States intervenes—as the United States has promised to do in the event serious hostile acts are initiated. An intense initial attack will further the enemy's goal. Attacking before the island's main supporter (the United States) can assist in its defense will maximize the effectiveness of the strike.

Simultaneity

A primary effect of the attack is to degrade the island's airfields and command and control facilities. The operational objective is to overrun island air defenses early. The goal is to maintain constant pressure, thus preventing the island from reconstituting air superiority.

Simultaneously, an attempt is made to cut the island's SLOCs. This is seen to be useful in weakening the island as the conflict continues, even if the tactic were unsuccessful in forcing capitulation. The island is particularly dependent on its SLOCs for fuel. The aggressor plans to declare an interdiction and launch an effort to destroy several merchant vessels before the United States can intervene. In the (likely) event capitulation does not occur early, the interdiction will be extended as part of a war of attrition.

Capitalizing on Asymmetries

Although the aggressor's air force is numerically superior to the island's air force in 2010, the aggressor cannot bring all of its aircraft to bear in any reasonable period of time. The problem is that the aircraft are widely dispersed and the command and control capability is undeveloped. The aggressor's only leverage is that, unlike the island, it can replace losses from out-of-theater. The island's qualitative advantages in aircraft and crew training offset the numeric disadvantage.

The aggressor plans to employ asymmetric warfare techniques developed in the last decade of the twentieth century. Key to its strategy is its relatively large and capable submarine force, its missile force (especially ballistic missile), and a limited electronic warfare (EW) capability.

The Aggressor's Asymmetric Advantages

Submarine Warfare: Beginning in the 1990s, partly as a result of the high-tech Iraq war, the enemy recognized the value of modern, capable forces, including submarines, and has since devoted considerable resources to modernize its forces. The submarine force, however, has been optimized for attacks against surface ships and not for antisubmarine warfare (ASW). In 2010, the island still cannot counter the enemy submarines with other submarines, surface ships, or aircraft. As a result, the enemy nation can apply pressure to the island nation's SLOCs for long periods without significant risk to its own submarine forces.

Missiles: The enemy nation has developed a daunting missile challenge in 2010 built on conventional theater ballistic missiles and land-attack cruise missiles. They offer a means to attack early those assets most directly relating to the island nation's ability to sustain defensive operations. Defense of more than a small fraction of the island nation against this threat is infeasible. Used in large numbers at the outset of a conflict, these missiles could gain the enemy country early air superiority over the island nation.

Electronic Warfare: The enemy nation has developed a significant EW capability against the island nation's warning radars, without which it cannot intercept attacking aircraft efficiently. Along with the aforementioned missile advantage, this capability could help the enemy nation achieve air superiority early in a conflict.

The Enemy View

A key problem for the aggressor in 2010 is the dispersion of its air forces and the lack of a modern command and control structure that can effectively mass airpower in a timely manner. It must also anticipate U.S. involvement in any conflict with the island. Once in the fight, U.S. forces can threaten much of the aggressor's navy. The aggressor, therefore, plans to move its navy into a defensive bastion to protect all of its high-value ships.

We assume U.S. forces are located just a few hundred miles from the enemy nation, and less than a thousand miles from the threatened island. U.S. Navy forces can be on the scene in about a day after getting under way. The fact that the United States can become involved this quickly influences the enemy's strategy.

RESISTANCE TO ANNEXATION

The island's strategic objective is to "hold on" against an anticipated massive enemy application of force early in any conflict. The aggressor hopes that its massive application of force will result in an early capitulation. This would be the worst possible outcome for the island as a nation, and therefore it must be prepared to weather such an attack. At a minimum, the island nation must plan to hold out until the United States intervenes.

Although the island cannot hope to defeat its enemy militarily, it can strive to fight to a draw, with the aggressor tiring of the conflict and seeking peace. At best, the aggressor will decide that the cost of continuing the conflict (a war of attrition) would outweigh any possible gain, thus ending the conflict under favorable terms for the island nation.

Operational Objectives

The island nation's primary objective is to maintain air superiority over its contiguous waters—at least up to the limits of the enemy's surface-to-air missile (SAM) envelope. This is paramount. It is vital to protecting SLOCs and ALOCs and deterring or defeating enemy assaults by sea or air.

An important weapon for maintaining air superiority in the island nation's arsenal is the F-16 fighter aircraft. Their pilots have been trained in the United States, and they get considerably more flight hours than their enemy counterparts. Consequently, the island has superior air force operational proficiency. This strength is enhanced by command and control capabilities considerably superior to the enemy's uncoordinated air force.

Geographically, the island's air superiority will cover all of the island and much of the waters between itself and the enemy, but it will not extend to the enemy coast. Aircraft attacking the island must emerge from overlapping SAM coverage areas before they can be engaged. However, the ALOCs on the island and lesser combatants can be protected against enemy surface attacks on shipping near the island.

Figure 2.1 illustrates the situation facing the island as it prepares to defend against an anticipated attack.

THE U.S. ROLE

U.S. naval forces are positioned to help the island improve its defensive posture against enemy missile attacks by intercepting missiles in flight. There is no desire for the United States to attack the enemy's territory. U.S. aircraft will position themselves to fill the gaps in the island's defense and thereby help ensure that the island

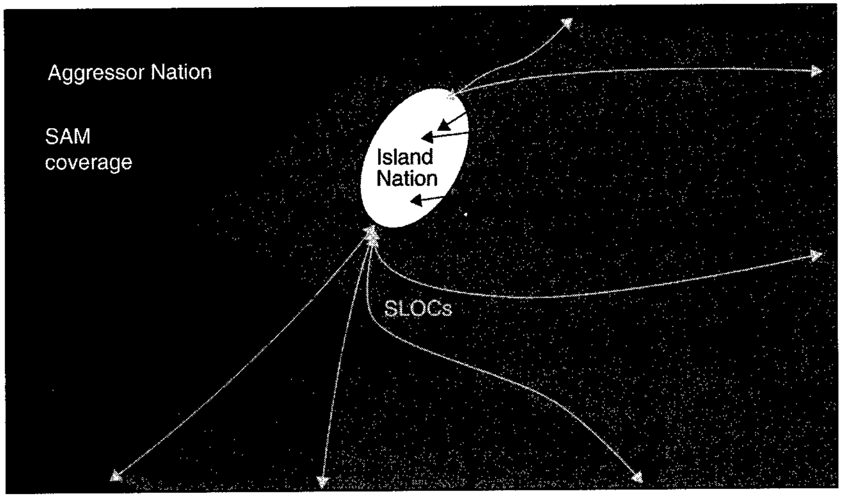


Figure 2.1—Theater of Operations

nation achieves its primary objective of maintaining air superiority over the island and much of the waters between itself and the enemy.

A consequence of the U.S. involvement will likely be to force the aggressor into a defensive posture, thus limiting its offensive options.

U.S. Air and Sea Operations

Initially the carrier battle group (CVBG) operating nearby will be positioned east of the island with MODLOC position placing it out of enemy reach.[1] It is joined by a second CVBG before the outbreak of hostilities.

Aegis cruisers will be assigned to ballistic missile defense duty off the island's two major ports, and SSNs will be assigned to attack enemy interdiction submarines. Figure 2.2 illustrates the disposition of a portion of U.S. naval forces in the theater at D-day.

[1] "MODLOC" stands for Miscellaneous Operational Details, Local Operations: fixed, geographically defined operating areas.

- **Air Superiority:** U.S. forces will help defeat raids across the waters between the island and the aggressor and kill leakers over the island either directly using its fighter aircraft or indirectly by providing command and control support.
- **Missile Defense:** Early on, the Aegis cruisers will provide Theater Ballistic Missile Defense (TBMD) over critical ports and airfields. Later in the conflict, U.S. forces will attack surface combatants who are equipped with Land-Attack Cruise Missiles (LACMs). The aggressor's intent to use its missiles early lends urgency to the latter mission.
- **Breaking the Blockade:** Enemy surface ships operating outside ports and bastions can be eliminated quickly. Nevertheless, these ships collectively threaten U.S. Navy forces in the area. A large, saturation ASCM attack would be particularly attractive to the aggressor. It would be difficult to coordinate such an attack, but it could succeed through force of numbers. The aggressor's interdiction effort will give its submarines freedom of operation.

RANDMR1449-2.2

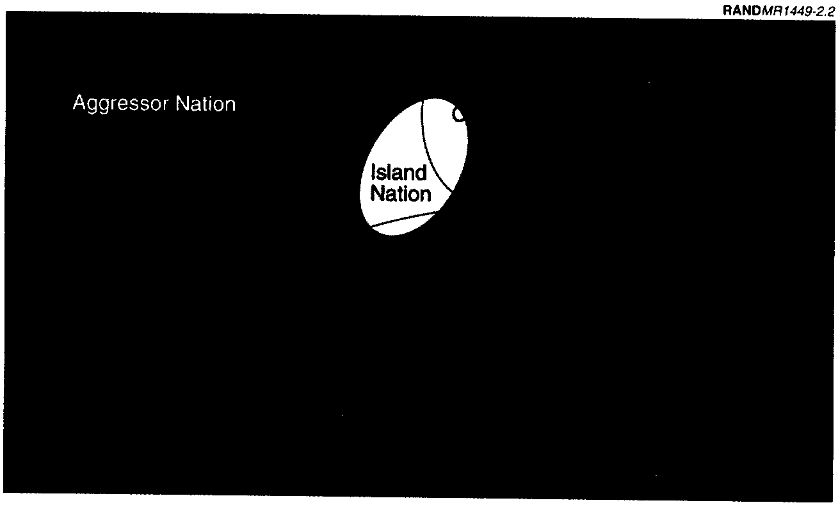


Figure 2.2—Disposition of U.S. Naval Force

Conditions around the island are expected to be poor for ASW, so relatively advanced threats like the improved Kilo will be hard to find.

- **Placing the Enemy on the Defensive:** U.S. presence in the conflict will force the enemy navy into a defensive posture. In 2010, the aggressor will have no counter for U.S. nuclear-powered attack submarines (SSNs), for example. At sea, the best destroyers available to the aggressor will be easy targets for a *Los Angeles*-class SSN. Consequently we would expect that enemy surface combatants would retreat to ports or bastions, thus preventing their certain destruction in open waters. The aggressor's surface, subsurface, and air platforms will be largely ineffective against modern U.S. SSNs. Consequently, defense in depth is the enemy's only option. It could interpose minefields, ships with active sonar, and submarines to try to stop a U.S. SSN. With surface combatants forced to retreat for self-protection and with forces committed to the defense of high-value units and systems, fewer capable combatants will be available to the aggressor for use against the island.

THE BASIS FOR ANALYSIS

Central to the analysis of vignettes derived from this and other scenarios is the effect of changed command and control systems and procedures on the outcome of the battle. Network-centric operations purport to improve combat operations. However, this is merely an assertion and therefore must be regarded as a hypothesis. However plausible it may sound, it requires rigorous assessment, and, to do that, a credible link between command and control systems and procedures and combat outcomes needs to be established.

In the next two chapters we attempt to do just that. We focus on the development of mathematical relationships that link network-centric operations, command and control, combat operations, and combat outcomes in the context of the scenario just described. In assessing network-centric operations and command and control procedures, we develop measures of performance. Assessing combat operations and combat outcomes is generally accomplished through the development of measures of combat effectiveness. In this work we have linked the two so that the effects on combat outcomes of variations in C4ISR procedures and processes can be assessed.

In developing the combined metrics, we rely on graph theory to assess the value of connectivity, information theory to assess the value of collaboration and the effects of knowledge, and traditional measures of combat to assess the value of combat power. It is important, however, that we emphasize that no claims are made concerning the "correctness" of these formulations. They must be treated as hypotheses subject to testing, validation, and calibration.

Chapter Three

CRUISE MISSILE AND BALLISTIC MISSILE DEFENSE

This chapter examines the information aspects of ship defense against ASCMs while those ships conduct TBMD. Overall, the defense problem is analyzed as a double-queuing problem. First, the launched ASCMs and ballistic missiles in a given time period, *T*, enter an initial engagement queue based on an assessment of the likelihood that cruise missiles will be a threat to the defenders (two Aegis cruisers) or that the ballistic missiles will be a threat to critical infrastructure targets. Second, if no interceptor missile defeats the incoming attack missiles, one of two things will occur: ASCM leakers will join a second queue to be "serviced" by the Close-In Weapon System (CIWS) on board the cruisers, or ballistic missile damage to land targets will be assessed.[1]

We begin by discussing the development of the "initial engagement queue" and the rate at which that queue is populated or the arrival rate of missiles for each time period. Next, we develop the appropriate "service" rates depending on the shooting policy established. Finally, we address the leaker or terminal queue.

[1] http://www.chinfo.navy.mil/navpalib/factfile/weapons/wep-phal.html. Phalanx provides ships of the U.S. Navy with a "last-chance" defense against antiship missiles and littoral warfare threats that have penetrated other fleet defenses. Phalanx automatically detects, tracks, and engages antiair warfare threats, such as antiship missiles and aircraft, while the Block 1B's man-in-the-loop system counters the emerging littoral warfare threat.

INITIATING EVENTS

Two Aegis cruisers are assigned to cover the area of operations as depicted in Figure 3.1 in order to defend against a likely enemy cruise and ballistic missile attack. Given their role in defending friendly territory, the cruisers are also likely to be targets and therefore they are prepared to defend against such an attack.

Although it is likely that other ships would be in the area of operations, for purposes of this analysis, we assume that only the two Aegis cruisers are involved in the attack and in the defensive operations.

Measures of Performance and Force Effectiveness

The Aegis cruisers have two (competing) missions: defend against cruise missile attacks against themselves and prevent enemy ballistic missiles from destroying key allied infrastructure targets. For both missions, the obvious measure of success is survivability; that is, *the fraction of the critical infrastructure targets that survive the attack and the "fraction" of the cruisers that survive the attack.* In the case of the cruisers, the "fraction surviving" may not be meaningful in that a

RANDMR1449-3.1

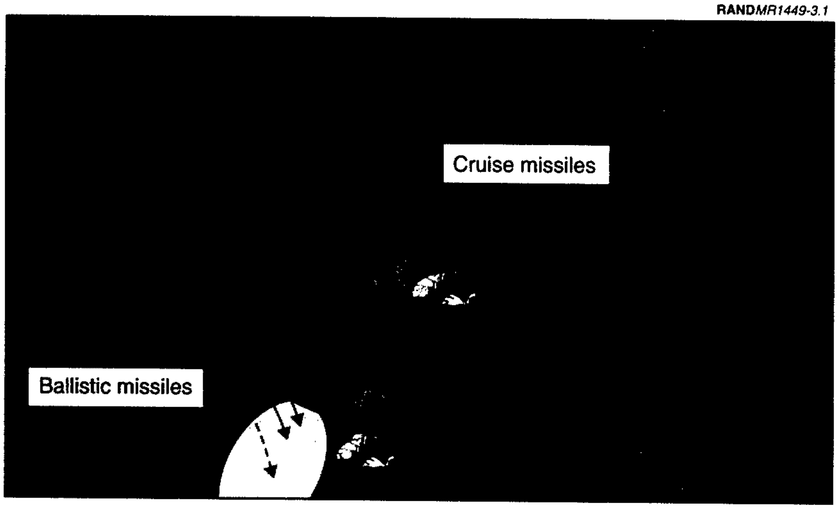


Figure 3.1—Coordinated Enemy Attack

single hit by a cruise missile is likely to result in damage sufficient to render the ship useless.

Given the two missions, priority is clearly given to defending the two Aegis cruisers. If they fail to defend themselves, they cannot conduct TBMD. Depending on the nature of the attack, this can pose serious problems for the defense of allied infrastructure targets.

Few uncertainties are considered in this analysis. We assume that the AN/SPY-1 radars on board the cruisers will detect and track all missiles the enemy is able to launch with certainty.[2] Only those missiles considered likely to hit infrastructure targets and the cruisers are considered a threat.

We further assume that through the Intelligence Preparation of the Battlespace (IPB) process, the size of the enemy missile attack inventory is known. It is also possible that the fixed launch sites would be known as a result of the same process. The locations of sea- or land-based mobile launch sites are not likely to be known. However, we assume air and sea supremacy, and therefore these are no longer a serious threat. The minimum time required to launch an attack can also be estimated. What is not known, however, is the attack distribution for ballistic missiles and cruise missiles—i.e., how the enemy will schedule the attack to ensure that the friendly infrastructure targets are destroyed while minimizing interference from the defending cruisers.

Knowing the attack distribution contributes directly to the allocation of missile interceptors and therefore to the effective defense of both the cruisers and the friendly infrastructure targets. Defenders may determine that they have ample defensive weapons, for example, and therefore respond more aggressively. A measure of performance therefore is *the degree to which the friendly commander "knows" the enemy's attack distribution.* Before the attack begins little is known, and at the end of the attack the distribution is known with certainty.

[2] The heart of the Aegis system is an advanced, automatic detect and track, multifunction phased-array radar, the AN/SPY-1. This high-powered (four-megawatt) radar is able to perform search, track, and missile guidance functions simultaneously with a track capacity of more than 100 targets. The computer-based command and decision element is the core of the Aegis combat system.

As the attack unfolds and the enemy completes its attack, more information is obtained allowing the friendly commander to increase his knowledge concerning the distribution of the remaining attack.

ALTERNATIVES

Network-centric operations include connectivity, equipment, and operating procedures (information and sensor grids). The emphasis here is on the operating procedures—i.e., the degree of cooperation between the two cruisers in servicing the targets. This in turn depends on the nature of the connectivity between the two and the command and control arrangements in place. In this simple arrangement, operations consist primarily of how the two cruisers function to accomplish the desired mission. For this study, we examine three alternatives: operations with divided duties, independent operations using a shared COP, and coordinated operations using CEC.

Cruiser Operations

The Aegis cruisers operate in pairs with one cruiser, $A^{(b)}$, directing its SPY-1 radar to detect and track ballistic missiles, while the other cruiser, $A^{(c)}$, directs its SPY-1 radar to detect and track ASCMs as depicted in Figure 3.2. This is necessary to ensure that both threats are covered given that both types of coverage cannot be provided simultaneously by a single radar.

Platform-Centric Operations—Divided Duties

In this case, the two cruisers operate almost autonomously (see Figure 3.3). That is, no mechanism on board either ship automatically shares information on the arriving threat and/or firing solutions and no central authority directs the defensive response. Control is decentralized and managed in the Command Information Center (CIC) and therefore each ship acts alone: one ($A^{(c)}$) against all incoming cruise missiles and the other ($A^{(b)}$) against all incoming ballistic

RANDMR1449-3.2

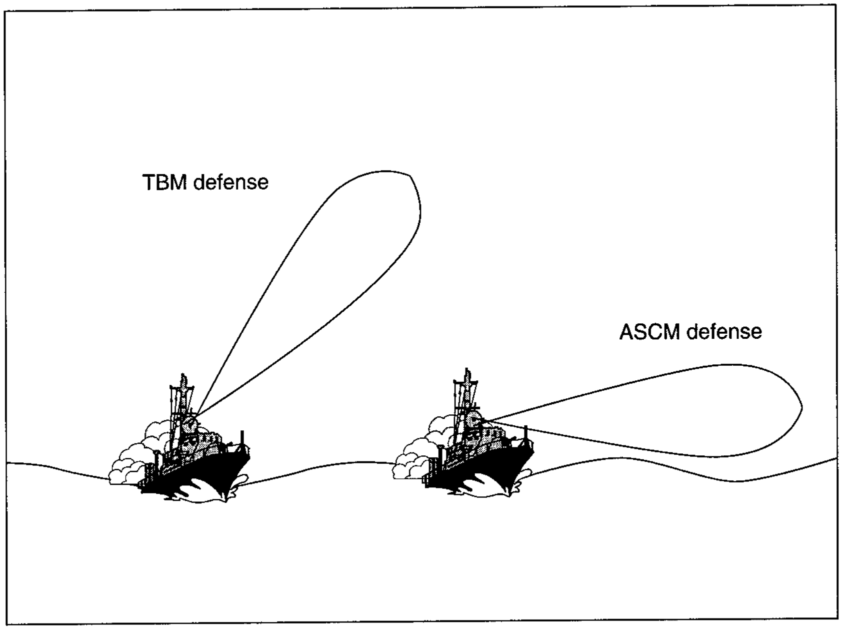


Figure 3.2—Cruiser Operations

RANDMR1449-3.3

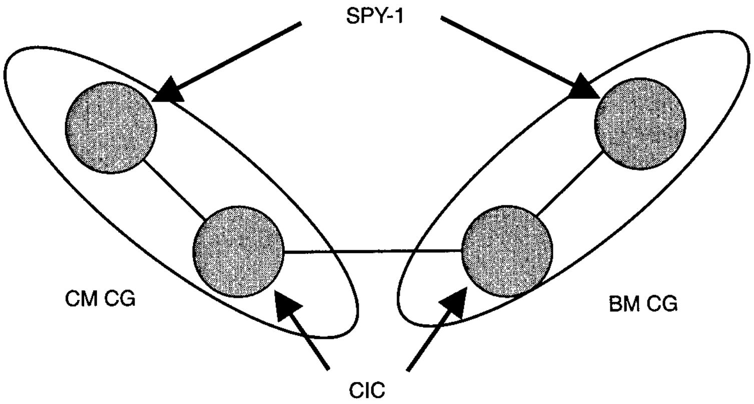


Figure 3.3—Divided Duties Connectivity

missiles.[3] Both Aegis ships employ a first-in-first-out (FIFO) queue-discipline policy for engaging incoming missiles. For cruise missiles, this means that self-preservation is collective. That is, the ship designated to intercept cruise missiles does not give itself priority against attack.

Both ships must take several decisions based on the situation they confront and the information available to them from organic and external sources. Not all of these decisions are modeled in this study. The description of the modeled decisions appears later.

- **The ballistic missile defense ship,** $A^{(b)}$, must prioritize ballistic missile threats. If it concludes that an enemy missile is not going to hit a high-value target, it may not defend against it. If it concludes that an enemy missile will impact a high-value target, it either chooses to engage it or may conclude that it will be defended by another system, such as Patriot, and therefore choose not to defend against it. If it concludes that an incoming enemy missile will impact a target no longer worth defending (because it was destroyed earlier), it will not defend against it. It must decide how many Standard missiles it is willing to assign against a given incoming enemy ballistic missile. If it appears that it could run out of defensive weapons before the ballistic missile attack ends, it must decide if that is a real problem and work to switch roles with the other cruiser (covered separately below). Although it has no inherent self-defense capability, it *can* decide how to operate so that the other ship can defend it.
- **The cruise missile defense ship,** $A^{(c)}$, must prioritize its response to cruise missile threats. It must decide between defending itself and the ballistic missile defense ship based on remaining inventories of anti–cruise missile (ACM) and anti–ballistic missile (ABM) weapons on board both ships. It must decide how many Standard missiles it is willing to assign to a given cruise missile as with the $A^{(b)}$ ship. If it appears that it could run out of defensive

[3] One or two Aegis ships could perform simultaneous cruise missile and ballistic missile defense. Use of two Aegis ships was selected for this analysis because of the more challenging command and control problem associated with using two ships and because two-ship defense was judged more appropriate to the projected threat. This arrangement should be viewed as a "first step" toward developing discrete, collaborative command and control metrics in a network-centric context.

weapons before the cruise missile attack ends, it must decide if it has a real problem and work to switch roles (covered separately below). It can also attempt to maneuver to make it easier to defend itself and the ballistic missile defense ship.

- **Role-switching decision:** The operational sequence for switching roles is illustrated in Figure 3.4. Once it has been determined that a reversal in roles is necessary (based on inventory levels of ACMs and ABMs on both ships), the ballistic missile defense ship "lowers" the regard of its SPY-1 radar to search for cruise missiles (Figure 3.3a). During this period, there is no ballistic missile

RAND*MR1449-3.4*

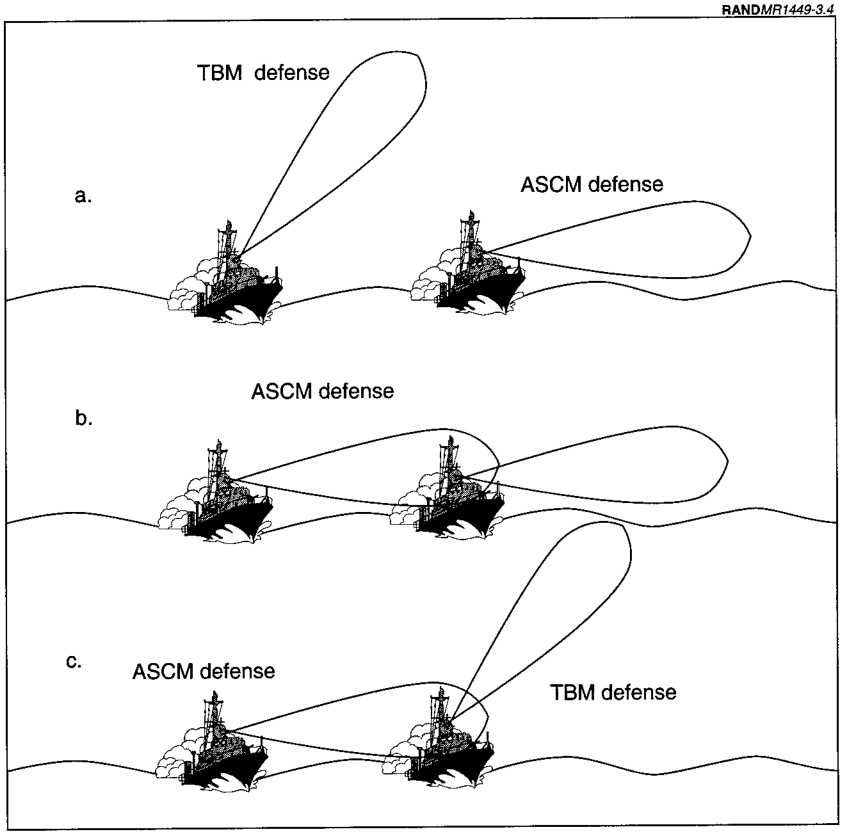


Figure 3.4—Role-Switching Operations

defense capability, meaning ballistic missile tracks built up may be lost. Once both ships have cruise missile tracks (i.e., once $A^{(b)}$ has cruise missile tracks), $A^{(c)}$ can raise the regard of its SPY-1 radar to detect ballistic missiles. Role reversal is complete when $A^{(c)}$ has built up ballistic missile tracks and can begin defending against them.

Except for a brief turnover period, divided duties operations means that only one ship can defend against cruise missiles at any time. Cruise missile saturation is relatively easy because only one ship's launchers are used to protect two ships. Cruise missiles that could be stopped by two ships become "too hard" for a single ship with a single geometry. The ballistic missile ship is unable to periodically step in to help the cruise missile ship. Similarly, ballistic missile saturation is difficult to prevent. To avoid running out a magazine the ships may have to swap roles, leaving a gap in ballistic missile defenses. After a switch, knowledge of which targets have been hit may disappear.

Network-Centric Operations—Shared COP

In the shared COP mode, both ships can see and defend against both incoming ballistic missiles and incoming cruise missiles (see Figure 3.5). We term this case network-centric because an understanding exists between the two ships concerning the nature of the attack. This implies greater connectivity than in the platform-centric case. Information on missile threat trajectories and arrival times is shared electronically, and in this sense the two ships can collaborate. As in the previous case, one ship ($A^{(b)}$) trains its SPY-1 radar to detect ballistic missiles and the other ($A^{(c)}$) to detect cruise missiles. Even though sensor information is shared, the two ships continue to operate independently: no cooperation or coordination takes place between the ships. However, both ships have cruise missile and ballistic missile defense responsibilities. As a result, poor "queue discipline" is likely in that both ships may engage the same missile or fail to engage a missile that with better coordination might have been engaged.

The decisions in this case center on how to ensure the optimal allocation of defensive weapons against both cruise and ballistic missiles

RANDMR1449-3.5

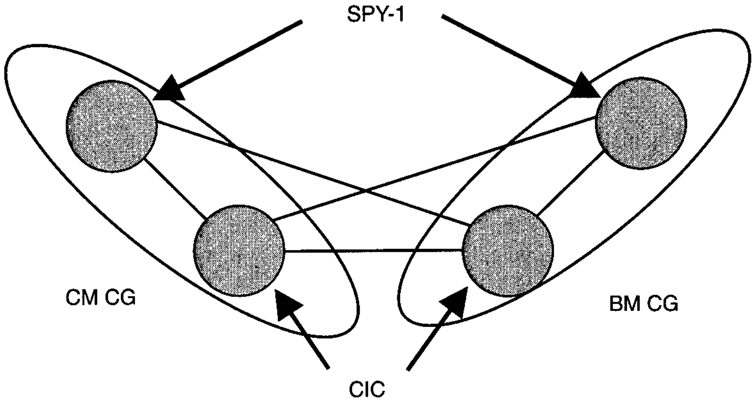


Figure 3.5—Shared COP Connectivity

given decentralized control.[4] The problem is complicated by the fact that either ship can defend against either type of threat. These decisions are described in more detail later. The decisions for both ships are:

- **Self-Protection:** The primary goal of both ships is survival. However, undue emphasis on self-protection means the other ship can be hit (possibly leaving the remaining ship more vulnerable). In addition, undue emphasis on protecting the two ships degrades defense against ballistic missiles. Each ship decides which of the incoming enemy missiles are easier for it to hit based on location and trajectory of the missile in relation to its own position. This sets up an attack priority. This can, of course, result in two ships attacking the same cruise missile target.
- **Ballistic Missile Interception:** Although the primary goal of the two cruisers is self-protection, their operational mission is to protect critical friendly infrastructure. In the absence of a cruise

[4] The term "optimal" is used here and throughout the text in the sense that major improvements can be realized.

missile threat, the same rules applied to cruise missile defense are applied to ballistic missile defense with the same possibility that both ships attack the same incoming enemy missile.

We would expect that, under these conditions, cruise missile and ballistic missile saturation would require about twice the arrival rate of the previous case. This is based on both ships' ability to engage cruise missiles as well as ballistic missiles. Given a target difficult for one ship and relatively easy for the other, there is a natural tendency for the shot to be "assigned" appropriately. Systematically reducing incoming missiles is not possible because the ships are unable to cooperate in any organized way. Without cooperation, if one ship gets into trouble, the other generally cannot step in quickly to help. Situational awareness is increased in this case, but the Guided Missile Cruisers (CGs) cannot affect all events they can see.

Network-Centric Operations—Cooperative Engagement

As in the previous two cases, one ship has its SPY-1 trained on incoming cruise missiles and the other on incoming ballistic missiles (see Figure 3.6). Now, however, both ships have access to complete defense solutions and the allocation of ships to targets is controlled centrally—by one of the two ships engaged in the operation. We depict a separate node for this additional function for the controlling commander. Not only connectivity is required in this case, but also automated systems to assess the relevant factors that go into making the best decision. Both ships have cruise missile and ballistic missile defense responsibilities as in the previous case.

The decisions in this case center on how to ensure the optimal allocation of defensive weapons against both cruise and ballistic missiles given *centralized* control and a richer shared COP. As in the previous cases, the descriptions of how the decisions listed here are implemented in the model follow later. The decisions for both ships are:

- **Cruise Missile Defense:** Single-authority decisions to engage incoming cruise missiles are made on the basis of which ship is closer to being overwhelmed. That is, if saturation of ship defenses is imminent, defensive efforts will shift from TBMD to ASCM defense. In this case, if one ship faces an imminent threat, defensive efforts will focus to defend it. Overall, priority is given

RANDMR1449-3.6

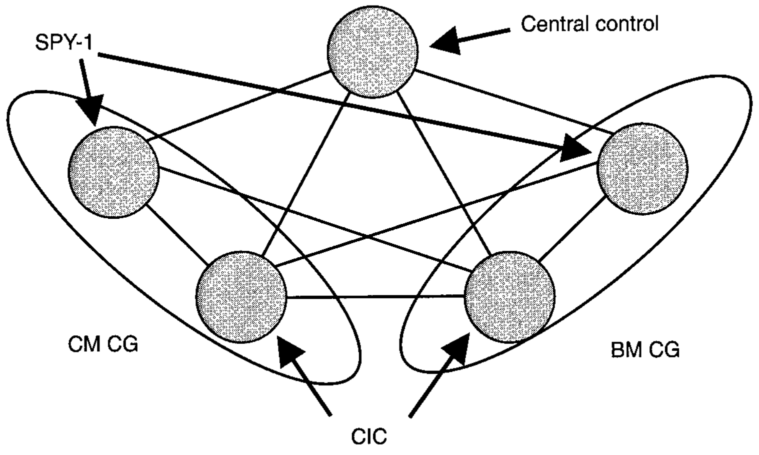


Figure 3.6—Cooperative Engagement Connectivity

to engaging cruise missiles, but now, the two ships cooperate to ensure that the most threatened ship is protected first. It may be necessary to prioritize protection of one ship over the other. A hit to the ship with the radar set for cruise missiles will leave the other ship completely unprotected for a short period, so it may be given higher priority.

- **Ballistic Missile Defense:** The single authority must prioritize the goals of self-protection, protecting the other ship, and protecting against ballistic missiles. Undue emphasis on ship protection can degrade performance against ballistic missiles. The optimal allocation of interceptors to incoming enemy ballistic missiles depends, in part, on the knowledge the central authority has concerning the distribution and projected size of the attack.

Both ships can defend against cruise missiles and against ballistic missiles, and they can cooperate and coordinate. Cruise missile saturation requires at least twice the arrival rate of the baseline case. Given a simultaneous need to engage an easy target and a hard one, an optimal decision may be made based on the relative position of the ships. Systematically reducing incoming missiles is now possible because of mutual cooperation. Similarly, ballistic missile saturation is at least twice as difficult for the reasons stated in the previous case. With cooperation, if one ship gets into trouble, the other can step in to help.

THE INITIAL ATTACK QUEUE

In any period, not all attacking cruise and ballistic missiles will be judged to be threats. Ballistic missiles not projected to damage predesignated critical infrastructure targets are not considered to be a threat—even though they may land on friendly soil. For this study, these targets are taken to be the airports of debarkation and seaports of debarkation. Cruise missiles not projected to damage the two Aegis cruisers are not considered to be threatening. The initial attack queue consists only of those missiles projected to hit critical infrastructure targets or the two Aegis cruisers.[5] The rate at which that queue is populated (the arrival rate) is therefore of interest and not the rate at which the missiles are detected by the Aegis radars.

For simplicity, we assume that only ballistic missiles are directed toward infrastructure targets and only cruise missiles are directed toward the Aegis cruisers. We further assume that Aegis cruisers are the only targets for the enemy cruise missiles. Other ships in the theater are not considered to be "in play."[6]

ARRIVAL RATES

Analysis of the value of network-centric operations begins with the average rate at which missiles arrive at the initial attack queue. This is taken to be an input. The ability of the enemy to effectively target friendly infrastructure with ballistic missiles and its ability to attack friendly ships, although important to the arrival rate as defined here, are not considered in this analysis. We assume a level of enemy capability and focus our attention on the queue itself. In a more de-

[5] This is based on the assumption that track and projection capability is sufficient to discriminate between threat and nonthreat missiles.

[6] These constraints can easily be relaxed. They are imposed here to allow for concentration on the problem of defending against the dual threat where the focus is on alternative command and control processes.

tailed simulation, the capability of the enemy to target friendly assets may be of interest. What is important here, however, is the ability of the defending Aegis cruisers to deal with a given threat.

The Attack Scenario

First, we assume that for the entire attack, the number of launched cruise missiles arriving is n_c and the number of ballistic missiles arriving is n_b. The duration of the attack is taken to be T minutes. During that interval, the arrival rate will vary. We assume that the missiles arrive in τ intervals each of which is t minutes in duration so that $T = \tau t$. We further define the average arrival rates per minute in time period i for the two types of missiles to be λ_{ci} and λ_{bi}. The total number of cruise missiles and ballistic missiles arriving in the attack (n_c and n_b) and the number of each type arriving in each time period are set parametrically. Therefore, the total number of each type of missile arriving in time period i is $\lambda_{ci} t$ and $\lambda_{bi} t$, and we have that the total attack sizes for the duration of the attack, T, are

$$n_c = \sum_{i=1}^{\tau} \lambda_{ci} t \text{ and } n_b = \sum_{i=1}^{\tau} \lambda_{bi} t .$$

Note that the average arrival rates in each time period are derived from the parametrically set number of missiles arriving in the period. Figure 3.7 illustrates a distribution of 300 cruise missiles and 50 ballistic missiles over $\tau = 5$ time periods. The shape of the distribution will depend on the enemy's attack strategy. If the objective is to saturate the allied defenses early, then the enemy might opt to coordinate the launch of a large part of its inventory to generate a large number of arrivals in the early periods. On the other hand, if the enemy's objective is to keep the cruisers busy while it pursues other offensive strategies, then a more uniform arrival rate is more likely.[7]

[7] Clearly, an "optimal" strategy would be to fire all missiles so that they arrive simultaneously and thereby saturate the friendly defenses. However, this is nearly impossible to accomplish.

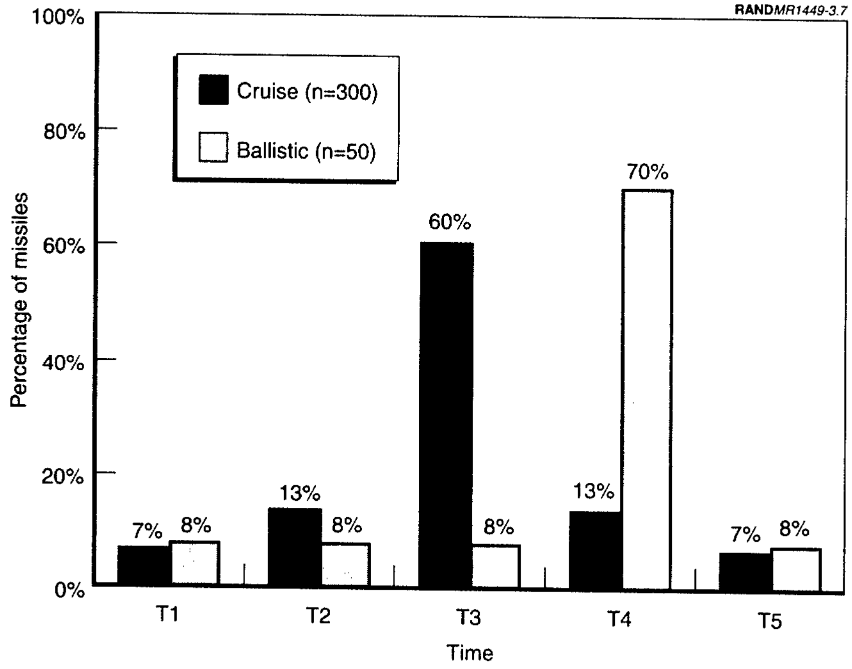


Figure 3.7—Enemy Missile Arrival Distribution

Additional Granularity

An important feature of the initial attack queue: it is "perishable." That is, service consists of destroying the missile in the queue or, in case of possibly repeated misses, absorbing its impact. A successful outcome, of course, is destruction of the missile, and therefore the sequence of arrivals is equally important. Because of this, we further subdivide each time period into subintervals with arrivals in each subinterval distributed according to a right-truncated Poisson. The right-truncated Poisson has a probability mass function of the form:

$$p[\mathrm{m}{:}\lambda] = \Phi \frac{e^{-\lambda}\lambda^{-m}}{m!}, \text{ for } m = 0,1,\ldots, g,$$

where m is the number of missiles arriving in the subinterval, $g = \lambda_c t$ or $g = \lambda_b t$ is the number of cruise missiles or ballistic missiles arriving in the time period, and

$$\Phi = \frac{1}{1 - \sum_{h=g+1}^{\infty} \frac{e^{-\lambda}\lambda^h}{h!}}.$$

Note that as $g \to \infty$, $\Phi \to 1$. Therefore,

$$\lim_{g \to \infty} p[\mathrm{m}{:}\lambda] = \frac{e^{-\lambda}\lambda_m}{m!},\ m = 0, 1, \ldots.$$

This is the standard Poisson distribution with mean equal to $\lambda = \lambda_c$ or $\lambda = \lambda_b$ for the given time period.

If the number of subintervals is s, then we can calculate the average number of missiles arriving in each subinterval of duration: $d = t/s$.

For example, suppose the average arrival rate for cruise missiles in a single time period is $\lambda_c = 3$ missiles per minute. If a time period is 5 minutes in duration, we can expect $g = 15$ missiles to arrive in that time. If we further assume that the period is subdivided into $s = 5$ subintervals, the average number of missiles that arrive in each of the 5 subintervals (each of which is $d = 5/5 = 1$ minute in duration) is $h = g/s = 3$. What remains is to calculate the fraction of the 15 missiles that arrive in each of the 5 subintervals.

One way to distribute the arrivals is to use the cumulative probability distribution:

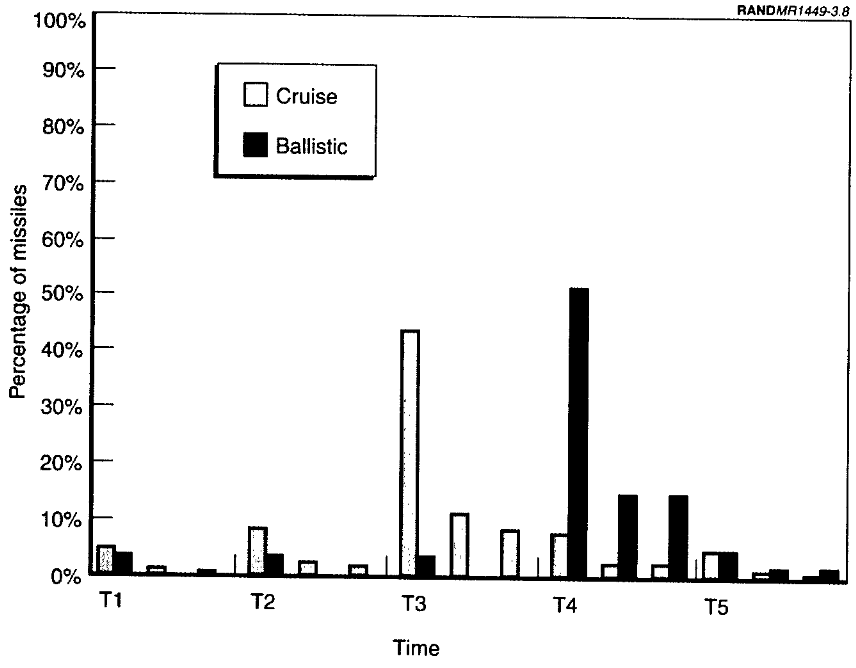
$$p(\mathbf{m} \le m{:}\lambda) = \sum_{i=0}^{m} p(\mathbf{m}{:}\lambda).$$

If there are s subintervals in a time period, with g arrivals, then the number of arrivals in each subinterval, h, is calculated to be as follows:

$$h_1 = P\left(\mathbf{m} \le \frac{g}{s}\right)g, h_2 = p\left(\frac{g}{s} < \mathbf{m} \le \frac{2g}{s}\right)g, \ldots, h_s = p\left(\frac{(s-1)g}{s} < \mathbf{m} \le g\right)g.$$

Figure 3.8 illustrates the further distribution of the missiles in Figure 3.7 using this methodology.

The subdivision of each interval allows us to model staggered arrivals throughout the period. This means that missiles will appear as targets for the Aegis interceptors at intervals. If we assume that within each time subdivision, incoming cruise missiles are detected at the same time, then the number of opportunities for the Aegis cruiser to



NOTE: In this example τ = 5, τ = 5 minutes, and therefore T = 25 minutes. For both cruise missiles and ballistic missiles, s = 3. For time period 3, for example, $g = \lambda_c\tau = 6 \times 5 = 30$ cruise missiles (approximately 60 percent of cruise missile inventory). The distribution to the subintervals is then $h_1 = 20$, $h_2 = 6$, and$h_3 = 4$.

Figure 3.8—Subinterval Enemy Missile Arrival Distribution

engage the missiles will depend on the time required to shoot a single missile and the shooting policy adopted by the cruiser.[8]

Allocation to Targets

Next, we address the distribution of arriving missiles to friendly targets. For simplicity, we assume that the distribution of missiles to targets is constant throughout all periods and subintervals. For cruise missiles, the n_c arriving missiles are allocated to the two defending Aegis cruisers, $A^{(c)}$ and $A^{(b)}$. If the proportion of incoming cruise missiles that will attack $A^{(c)}$ is $0 \le \alpha \le 1$, then the total number of incoming cruise missiles that will attack each cruiser is αn_c to $A^{(c)}$ and $(1-\alpha)n_c$ to $A^{(b)}$.[9]

The arriving ballistic missiles are allocated to infrastructure targets much in the same way, the difference being that there may be more infrastructure targets to be defended. In this case, we let ω_i be the fraction of incoming ballistic missiles, n_b, targeted against infrastructure target i, where

$$\sum_{i=1}^{\eta} \omega_i = 1$$

and η is the total number of infrastructure targets at risk. Again, we assume that the distribution of ballistic missiles to infrastructure targets is constant throughout all attack periods.

SHOOTING POLICY

The "shooting" policy affects the degree to which the weapon inventory on board the cruisers is depleted. In this work, we postulate three policies: shoot only, shoot-look-shoot, and shoot-look-salvo 2. We explain each of these next, but reserve explanation of their implications on success to later.

[8] This is discussed later.

[9] We avoid the term "allocated" because such fine precision given the operational proximity of the two ships is not possible. This therefore is a modeling artifact.

- **Shoot Only:** This is the simplest policy. As threat missiles present themselves, one or both of the ships launch a counter missile. In case of a miss, the target missile is considered a leaker. No further attempt is made to engage it with counter missiles.
- **Shoot-Look-Shoot:** In this case, one or both of the cruisers will fire against a target missile. Next, the radar tracking the missile will determine if the engagement was a success. If not, a second shot will be fired. If the second shot misses, the target missile is again considered a leaker and no further attempt is made to engage it with counter missiles.
- **Shoot-Look-Salvo 2:** This last case begins as in shoot-look-shoot, but instead of firing just one counter missile after a miss, two are salvoed. If the salvo misses, the target missile is again considered a leaker and no further attempt is made to engage it with counter missiles.

Because there may be insufficient time to fire the "postlook" shots in the shoot-look-shoot and shoot-look-salvo 2 modes, we may also explore intermediate cases. If γ is the fraction of times that post-look shots are fired given that the "look" has been executed and it is determined that the first shot failed to intercept the incoming missile, then the total number of shots taken is $(1 - \gamma) + \gamma S$, where $S = 2$ for the shoot-look-shoot policy and 3 for shoot-look-salvo 2 policy.

SERVICE

For one cruiser, the mean rate at which attack missiles can be serviced (the firing rate) is μ missiles per minute.[10] Service, in this case, has several components. Three prominent ones are missile/launcher test, missile preparation, and flight to target. Each consists of a time delay based on other factors. The first two depend largely on the level of automation in testing, time required to load target data into the missile, and time to "warm up" subsystems. Flight to target depends on the speed of intercept and the speed of attacking missile.

[10] For simplicity, we assume the cruisers service targets at the same rate—on average.

The procedural factors affecting the service rate reflect the quality of command and control in place, and therefore modifications should be made parametrically to assess the impact on the success of the operation. Delays stemming from weapon systems operating methods are considered fixed for this analysis. However, insights might be gained concerning possible weapon systems improvements.

If we let τ_1 be the mean time to prepare a launcher, τ_2 the mean time required to launch the intercept, and τ_3 the mean time to fly out to the target, then the total mean service rate for each cruiser is:

$$\mu = \frac{1}{\tau_1 + \tau_2 + \tau_3}.$$

Service is complete when the incoming attack missile and the defending missile "meet."[11]

SURVIVABILITY

The survivability of the defending Aegis cruisers depends on their ability to engage incoming cruise missiles, their firing rate, and the ability of the terminal defenses (CIWS) to destroy terminal leakers. The firing rate can be thought of as the "service rate." When the arrival rate exceeds the service rate, then the system becomes "saturated." Whether because of intercept failure or saturation, cruise missiles not destroyed become "leakers." In both cases, the leakers join a second queue to be serviced by the CIWS. The implications of this are discussed below.

Leakers

We let p_c be the *constant* single-shot probability that an intercept from the Aegis cruiser kills an incoming cruise missile. This ignores the variations in threat weapons (such as stealthy missiles). We use

[11] As the battle proceeds, the relative length of these times will vary. Initially, all targets will be engaged at maximum range, and therefore fly-outs will be lengthy. However, later in the fight we expect that the fly-out time would be significantly reduced because targets would be engaged closer in. In any case, τ_3 will likely always be larger than τ_1 and τ_2.

this kill probability only when the threat missile is between the maximum and minimum engagement range as discussed below. As a result, p_c is independent for multiple defensive shots, and the effective kill probability will depend upon the shooting mode and p_c. For example, if $p_c = 0.7$, the shooting mode is "shoot-look-shoot," and only one ship engages the incoming missile, then the effective probability that a friendly interceptor will kill an enemy cruise missile is $P_K = 2p_c - p_c^2 = 0.91$, and, therefore, the probability that the attacking missile survives (becomes a "leaker") is $P_L = 0.09$.[12] In addition, the expected number of intercept missiles required to achieve this probability is $E_f = 2 - p_c = 2 - 0.7 = 1.3$ missiles.[13] Table 3.1 summarizes the effective kill probabilities and the expected number of missiles fired for each shooting mode.

Table 3.1

Effective Kill Probabilities

Mode	First-Shot Kill Probability	Second-Shot Kill Probability	P_K	Expected Shots Fired (E_f)
		One Ship Engaged		
Shoot	p_c	NA	p_c	1
Shoot-look-shoot	p_c	$(1 - p_c) p_c$	$1 - (1 - p_c)$	$2 - p_c$
Shoot-look-salvo 2	p_c	$(1 - p_c)[1 - (1 - p_c^2)]$	$1 - (1 - p_c)^3$	$3 - 2p_c$
		Two Ships Engaged		
Shoot	$1 - (1 - p_c)^2$	NA	$1 - (1 - p_c)^2$	2
Shoot-look-shoot	$1 - (1 - p_c)^2$	$(1 - p_c)^2[1 - (1 - p_c)^2]$	$1 - (1 - p_c)^4$	$4 - 4p_c + 2p_c^2$
Shoot-look-salvo 2	$1 - (1 - p_c)^2$	$(1 - p_c)^2[1 - (1 - p_c)^4]$	$1 - (1 - p_c)^6$	$6 - 8p_c + 4p_c^2$

[12] The probability of kill on the first shot is p_c and the probability that the target is killed on the second shot (i.e., the first shot misses and the second hits) is $(1 - p_c) p_c$. The effective probability then is $P_K = p_c + (1 - p_c)p_c = 2p_c - p_c^2$.

[13] Three possible events exist: (1) the incoming missile is destroyed on the first shot with the expectation of $1 \times p_c$ missiles fired, (2) the first shot misses and the second intercepts the missile with the expectation of $2(1 - p_c) p_c$ missiles fired, and (3) both shots miss with the expectation of $2(1 - p_c)^2$ missiles fired. The sum of these is $E_f = 2 - p_c$. This methodology is used to calculate the other expected values in Table 3.1.

In general then, the expected number of leakers in any period i is $L_i = P_L \lambda_{ci} t$, where $P_L = 1 - P_K$. This is the number that enters the terminal queue in the period. The distribution allocated to each cruiser is determined by the apportionment factor, α. This is discussed more fully below.

Saturation

Typically, in queuing models, saturation occurs whenever the arrival rate exceeds the service rate. In this application, saturation would occur whenever the rate at which enemy missiles arrive exceeds the rate at which the Aegis cruisers are able to defend against them. Although this is true in a sense, the problem is a bit more complicated because this is not a steady-state problem.

Enemy missiles are only vulnerable to friendly intercept with Standard missiles during a narrow window of opportunity as depicted by the shaded ring in Figure 3.9. If this opportunity is missed, the second line of defense is the CIWS depicted by the inner circle. The time-elevation graph in Figure 3.9 illustrates a notional flight with the times depicted as dotted lines. The times are:

- t_0: Time of enemy launch.
- t_1: Time enemy missile detected.
- t_2: Earliest time missile can be engaged with Standard missile.
- t_3: Latest time missile can be engaged with Standard missile.
- t_4: Earliest time missile can be engaged by CIWS.
- t_5: Impact time.

We assume that a Standard missile is launched when a single enemy missile heading toward the defending ship is detected—i.e., service begins at t_1. This means that the friendly force has a maximum of $t_3 - t_2$ minutes to engage the enemy missile. In general, the following condition must hold for a successful intercept:

$$t_2 \le t_1 + \frac{1}{\mu} \le t_3 ,$$

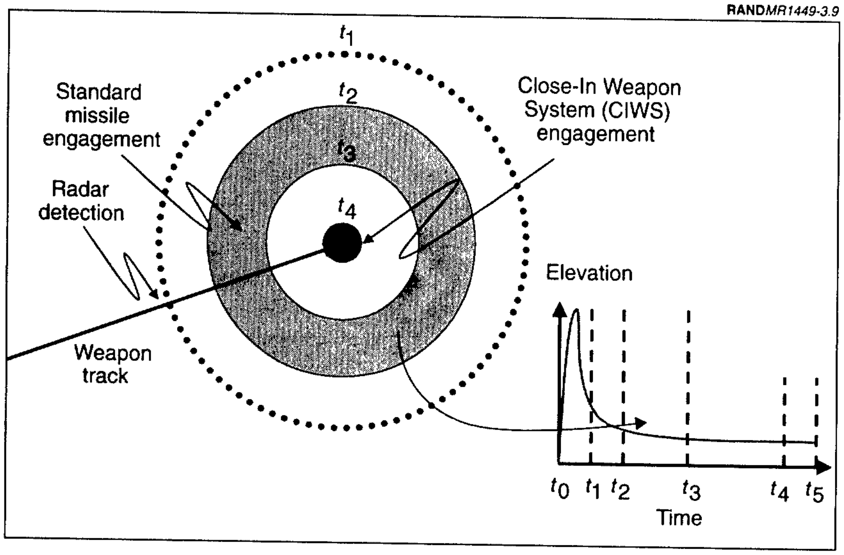

RANDMR1449-3.9
t_1
t_2
t_3
t_4
Standard missile engagement
Radar detection
Weapon track
Close-In Weapon System (CIWS) engagement
Elevation
t_0 t_1 t_2 t_3 t_4 t_5
Time

Figure 3.9—Cruise Missile Engagement Zones

where μ is the service rate as described above. For practical purposes, we can assume that $t_1 + 1/\mu \geq t_2$—i.e., it is unlikely that an intercept's launch time will be set such that it will intercept the enemy missile outside its effective range. Consequently, if h enemy missiles are detected at time t_1 (average arrival rate in a subinterval), we must have that:

$$h \leq \frac{t_3 - (t_1 + 1/\mu)}{\delta},$$

where δ is the time required to prepare the launcher for a subsequent launch: $\delta = \tau_1 + \tau_2$.[14] Hence, when the arrivals, h, exceed the service rate or when

[14] It might be argued that these times are insignificant when compared to the fly-out time and therefore in low-resolution models they may be neglected. We retain them here for completeness.

$$h > \frac{t_3 - (t_1 + 1/\mu)}{\delta},$$

we have

$$h - \frac{t_3 - (t_1 + 1/\mu)}{\delta}$$

enemy missiles that cannot be serviced in the subinterval.[15]

Because the enemy attack occurs over several of the subintervals, the average number of missiles the friendly commander must service is the average arrival rate for the subinterval plus the average not serviced in the previous subinterval. Furthermore, because the attack queue is FIFO (old targets must be serviced first), the additional enemy missiles left to be processed in the next time interval shrink its length. The implication of this is taken up next.

Recall that each subinterval is $d = t/s$ minutes long; therefore, the number of missiles that can be serviced in any subinterval is d/δ. This is based on the assumption that the second and subsequent missiles can be launched before the previous missile arrives on target. In other words, we need not consider fly-out times. Intercepts are launched at intervals of δ minutes.

The reduction in the length of the current interval occasioned by unserviced missiles is summarized in Table 3.2. Both the case where unserviced missiles are present and where they are not present have implications for the number of missiles "carried over" to the next subinterval.

In the table, the quantity:

$$\frac{t_3 - (t_1 + 1/\mu)}{\delta}$$

[15] Note that we do not refer to these as "leakers." The term "leaker" refers to *any* enemy missile not intercepted—including misses.

Table 3.2

Missiles Carried Over

		Missiles "Carried Over"
Case I: No unserviced missiles $h_i \le \frac{t_3 - (t_1 + 1/\mu)}{\delta}$	All missiles serviced in subinterval: $h_i \le \frac{d}{\delta}$	None
	Some missiles not serviced in subinterval: $h_i > \frac{d}{\delta}$	$h_i - \frac{d}{\delta}$
Case II: unserviced missiles present $h_i > \frac{t_3 - (t_1 + 1/\mu)}{\delta}$	All missiles that can be serviced will be serviced in the subinterval: $\frac{t_3 - (t_1 + 1/\mu)}{\delta} \le \frac{d}{\delta}$	None
	Some "serviceable" missiles are not serviced in the subinterval: $\frac{t_3 - (t_1 + 1/\mu)}{\delta} > \frac{d}{\delta}$	$\frac{t_3 - (t_1 + 1/\mu) - d}{\delta}$

is the number of enemy missiles that will be serviced in the subinterval.

In addition to varying the probability that an incoming enemy missile will be destroyed, the shooting policy also affects the number of enemy missiles that can be engaged in a subinterval. The quantities depicted in Table 3.2 reflect a shoot-only policy. For the shoot-look-shoot and the shoot-look-salvo 2 policies, the time required to prepare launchers for subsequent attacks increases to 2δ and 3δ, respectively. The "look" portion of the process is considered to be instantaneous in that the incoming missile is being tracked in real time and therefore a miss will be noted immediately. In the shoot-look-shoot case, a second intercept will be fired and therefore two launch preparations are required for each missile attacked. For the shoot-look-salvo 2 case, three missiles are fired.

Although saturation can occur as a result of the ballistic missile attack against infrastructure targets, the real concern is saturation from the cruise missile attack. We assume that survivability of the Aegis cruisers takes precedence over survivability of the infrastructure targets—not because the infrastructure targets are less important, but rather because with the loss of the cruisers no further defense is possible.

THE TERMINAL DEFENSE QUEUE

As mentioned earlier, all cruise missile that are not successfully engaged using Standard missiles (as a result of misses or defense saturation) join the terminal defense queue to be serviced by the CIWS.[16] The cruise missile arrival rate during any time period for the terminal queue is equal to the average number of leakers in that period. As mentioned earlier, the number of leakers in a period, L_i, depends on the shooting policy, the engagement procedures (one or two ships firing independently), and the degree of network-centricity. The proportion of terminal leakers allocated to each of the Aegis cruisers is αL_i for cruiser $A^{(c)}$ and $(1 - \alpha)L_i$ for cruiser $A^{(b)}$.

We now let p_d be the single-shot probability that an enemy cruise missile will damage an Aegis cruiser and we let p_a be the average level of damage required to disable the cruiser. By "damage" to the cruiser, we mean that its ability to engage attacking missiles is impaired by the fraction p_d and by "disable," we mean that its ability to engage cruise missiles has been lost. When the accumulated damage exceeds p_a, we assume the ship can no longer engage attacking missiles. We let N_L represent the number of leakers required to disable an Aegis cruiser. The expected fraction of damage caused by the N_L attacking missiles follows a binomial distribution so that if $p_a = 1-(1-p_d)^{N_L}$, then the expected number of leakers required to disable an Aegis cruiser is:

$$N_L = \frac{\ln(1-p_a)}{\ln(1-p_d)}.^{17}$$

[16] We assume that there is no terminal defense queue for ballistic missiles aimed at infrastructure targets.

[17] From *SABER/SELECT (SABSEL) and Weapons Effects Data Base (WEDB) User's Manual*, U.S. Air Force.

If we let p_e be the probability that an incoming missile escapes the CIWS, then the combined probability of a leaker is $P_L = P_L\, p_e$. Suppose we consider a sequence of attacks that each result in a probability of a leaker being P_L'. The number, X, of enemy cruise missiles required to achieve N_L successful leakers has a negative binomial distribution:

$$f(x{:}N_L,P_L') = \binom{x-1}{N_L-1} P_L'^{\,N_L}(1-P_L')^{x-N_L} \quad x = N_L, N_L+1, N_L+2, \ldots,$$

with mean $N_L(1 - P_L')/P_L'$. For example, if we let the single-shot probability of damage be p_d = 0.6, and let the fraction of damage required to disable the cruiser be p_a = 0.25, then the expected number of leakers required to disable the cruiser is:

$$N_L = \frac{\ln(1-.25)}{\ln(1-.6)} = 0.3140.$$

This means that with a shoot-look-shoot policy, the expected number of arrivals required to yield enough leakers to disable the cruiser (given the single-shot kill probability of an interceptor p_c = 0.7 and the probability that an attacking missile escapes the CIWS is p_e = 0.3) is:

$$\frac{N_L(1-P_L')}{P_L'} = \frac{N_L(1-p_eP_L)}{p_eP_L} = \frac{(.3140)(.91)}{(.3)(1-.91)} = 10.6.$$[18]

UNCERTAINTY AND KNOWLEDGE

The AN/SPY-1, the multifunction phased-array radar at the heart of the Aegis system, can detect and track incoming missiles with considerable accuracy. We therefore assume that the probability of de-

[18] The result is, of course, purely statistical. This expected value calculation does not take into account that a cruise missile cannot damage more than one ship. At least one cruise missile hit is required to disable one Aegis cruiser. Under the condition that the damage inflicted by a single cruise missile hit is expected to be disabling $(p_d)(p_a)$, N_L should be set to 1.0.

tection for any enemy missile is 1.0 and that the detecting cruiser knows the enemy missile's location, speed, and trajectory at all times. We also assume that the friendly decisionmakers have accurate information regarding their own inventories and capabilities. The only thing not known about the enemy attack, therefore, is the attack distribution—that is, when the main effort of the attack will arrive or how long it will last. We do assume that the friendly forces know the enemy's missile inventories and launch capabilities. Although this offers no information on the attack distribution, it does establish an upper bound on the attack size.

Gaining knowledge of the attack distribution means obtaining reliable estimates for the arrival rates, λ_{bi} and λ_{ci}, in Figure 3.7. These may be obtained through intelligence sources prior to the attack and from other sensors (other ships in the area; intelligence, surveillance, and reconnaissance—ISR—aircraft; etc.) during the attack. Knowing the character of the attack in a subinterval allows for a more optimal response. How this knowledge affects the cruiser and infrastructure survival rates is discussed below.

Uncertainty

For each type of missile (ballistic missiles and cruise missiles), we assume that the size, *n*, of the enemy missile inventories is known. Therefore, in the absence of any information, the arrival rate in each of the subintervals is estimated to be $\hat{\lambda}_i = n/T$.[19] With perfect information, the estimate is the true value, or $\hat{\lambda}_i = \lambda_i$. We assume that the fraction of remaining missiles that will arrive in period *i* is a random variable, *x*, with a beta distribution[20] as depicted in Figure 3.10.

The beta probability density has the form:

$$f(x;\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}, \quad x \in [0,1]$$

[19] We drop the *c* and *b* subscripts. The analysis is the same for both.

[20] Although the actual missile arrivals distribution is discrete (arrival counts are integer values), we are able to use the continuous beta distribution since our analysis is performed in an expected value setting.

with mean:

$$E(x)=\frac{\alpha}{\alpha+\beta}$$

and variance:

$$V(x)=\frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}.$$

For $\alpha = \beta = 1$, the well-known uniform distribution results reflecting maximum uncertainty. For α, $\beta > 1$, the distribution has a mode:

$$\frac{\alpha-1}{\alpha+\beta-2}.$$

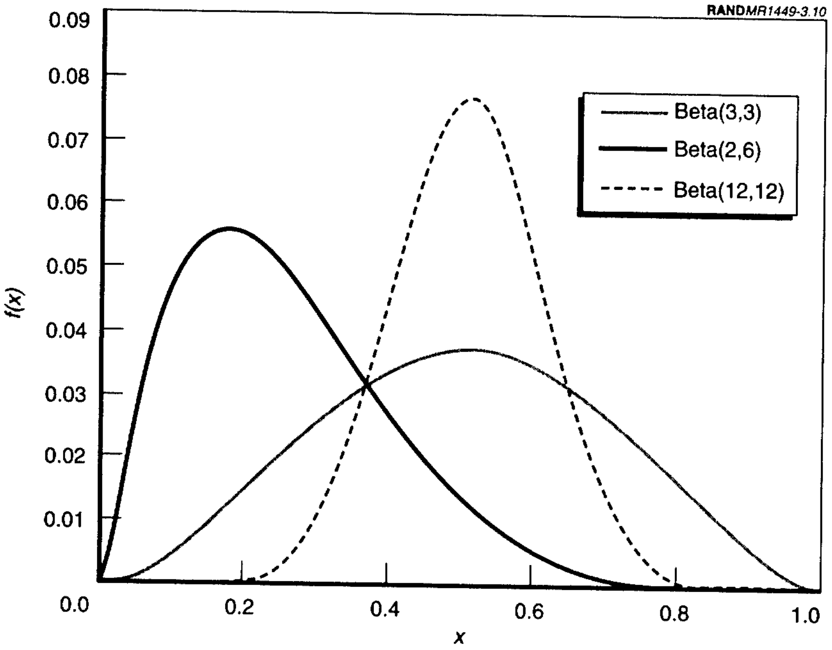


Figure 3.10—Arrival Rate Uncertainty

For purposes of this analysis, we consider only those distributions for which $\alpha,\ \beta \geq 1$.

The maximum number of arrivals in any time period, $i = 1,2, \ldots, \tau$, is

$$q_i = n - \sum_{j=1}^{i-1} t\lambda_j .$$

That is, the worst case is that all remaining missiles arrive simultaneously. Although not a practical consideration, it does provide an upper bound for the probability distribution. In the subsequent discussion, we drop the subscript *i*. It is understood that *q* refers to the remaining inventory of enemy missiles at the end of $i - 1$ subintervals.

The arrival rate in the current time period therefore is $\lambda = qx$, where *q* is the known inventory of remaining missiles.[21] If $E(x) = \xi$, then the expected arrival rate in the current time period is $E(\lambda) = qE(x) = q\xi$. Since ξ is the actual fraction of the remaining inventory scheduled to be launched in the current period, we need to choose the parameters of the beta distribution, α and β, such that

$$\frac{\alpha}{\alpha+\beta} = \xi .$$

However, because an infinite number of combinations of α and β can yield an unbiased estimate, we choose the appropriate values under the constraint that $\min(\alpha,\ \beta) \geq 1$ (ensuring that a mode exists) and such that the resulting variance achieves a "target value" $V_0(x)$. The target variance reflects the information quality, *Q*, associated with the sensor suite used to produce the estimate of missile arrival rate for the current period. For purposes of this discussion, information quality is the degree to which the information is current, correct,

[21] Note the fact that the random variable *x* is the fraction of remaining missiles that will arrive in this period implies that *x* is really a fractional arrival rate—i.e., the fraction arriving per minute.

and complete. Therefore, we set $0 \leq Q \leq 1$, where $Q = 1$ implies the information has maximum quality.[22]

Information Entropy

To assess the degree of knowledge present in a density, such as the one just described, we employ the concept of *Information entropy* or *Shannon entropy.* Information entropy is a measure of the average amount of information in a probability distribution and is defined as:

$$H(x) = -\int_{-\infty}^{\infty} \ln[f(x)] f(x) dx .^{23}$$

Information entropy is based on the notion that the amount of information in the occurrence of an event is inversely proportional to the likelihood that that event will occur. Thus there is no information in Orphan Annie's declaration that "the sun will come up tomorrow" whereas there is considerable information in the realization that an individual has won the national lottery. Because entropy is an expected value, it is also referred to as the average information in a probability density.

Knowledge

The distribution in Figure 3.10 is completely defined by the maximum time period arrival rate, q, and the mean arrival rate, $\lambda = q\xi$. From this we can calculate the information entropy, or the uncertainty in the distribution:

$$\begin{aligned} H(x) &= -\int_{x=0}^{1} f(x) \ln f(x) dx \\ &= \ln[B(\alpha,\beta)] - (\alpha - 1)[\psi(\alpha) - \psi(\alpha+\beta)] - (\beta - 1)[\psi(\beta) - \psi(\alpha+\beta)], \end{aligned}$$

[22] See Appendix A for a more thorough discussion of "target variance." For a more complete discussion of information quality, see Perry, Signori, and Boon (2001).

[23] Actually, because entropy is really a statistical expectation, the quantity should be $E[\ln(f(t))]$. However, in most texts this is shortened to $H(t)$ and we adopt this convention in this report. See Shannon (1948, pp. 379–423 and 623–556).

where $\psi(c)$ is the first derivative of Euler's gamma, and

$$B(p,q)=\frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)}.^{24}$$

We can create a mapping of entropy onto a [0,1] knowledge scale by selecting an upper bound on the entropy associated with the fraction, x. Before proceeding, however, we note that the uncertainty associated with the fraction of the remaining missiles arriving in the current period is equivalent to the uncertainty associated with the estimated arrival rate, λ, or $H(\lambda) = H(x)$.

The upper bound for $H(\lambda)$, denoted $H^*(\lambda)$, occurs when $\alpha = \beta = 1$. That is, maximum entropy occurs when uncertainty is maximized. In this case, therefore, we have that $H^*(\lambda) = 0$, a natural upper bound. A lower bound is also needed. However, minimum entropy occurs when the variance is minimized or when α and β are very large so that $H(\lambda) \to -\infty$. For practical purposes, we set this to be $\alpha = \beta = 12$ for which $H(\lambda) = -32.3192$.[25] We can define knowledge, therefore, as:

$$K(\lambda)=1+\frac{H(\lambda)-H_{\min}(\lambda)}{H_{\min}(\lambda)}=\frac{H(\lambda)}{H_{\min}(\lambda)}=\frac{H(\lambda)}{-32.3192}.$$

Note that the maximum time period arrival rate, q, is determined by the known enemy missile inventory, n, and the attack history. A natural maximum value for q therefore is the known enemy missile inventory. This presupposes, of course, that the arrival rates for all preceding periods were 0 and that the entire inventory will arrive in the next time period.[26]

In this form, knowledge is then used to influence the decisions taken subsequently and the outcome produced, as described below. First,

[24] See Appendix A for details concerning the computation of this quantity.

[25] See Appendix A for a more detailed treatment.

[26] This also ignores the fact that if the arrival rate up to now is 0, it is difficult to maintain that the attack has started!

however, we assess the effects of collaboration and network complexity.

COLLABORATION

Collaboration is a process in which individuals work together to achieve a common goal. It is important because it enhances the degree of shared awareness in a group focused on solving a specific problem or arriving at an agreed decision. Several reasons point to why collaboration might be expected to improve the degree of shared awareness, including the potential for increased sharing of information and experience as well as synergy of inference. However, other factors can degrade performance, such as disruptive interactions, misunderstandings, or overvaluing a particular point of view because of the persuasiveness or authoritarian role of an individual team member. For this reason, the opportunity to collaborate can both add to and detract from effective combat operations. Here, we treat the contributions only, but in varying degrees. We postpone a discussion of the negative effects for future research.[27]

In general, as the opportunity for a decision team to collaborate increases (more connections), the better the decision is—provided that the quality of the collaboration is good. The quality of human collaboration can depend on several factors, among which are the experience of the team, the amount of time they have been working together, the procedures in place to facilitate collaboration, the personalities of the individual members, and the knowledge the team members possess about the critical element(s) of the operation. [28] Here we deal primarily with collaboration among automated systems—compressed time scales might not accommodate human interactions.

Figure 3.11 collects the three operating procedures described above for reference. The degree of collaboration and the complexity of the network vary considerably among the three.

[27] For a fuller discussion of collaboration and shared awareness, see Perry, Signori, and Boon (2001).

[28] See, for example, Wegner (1987, pp. 185–208).

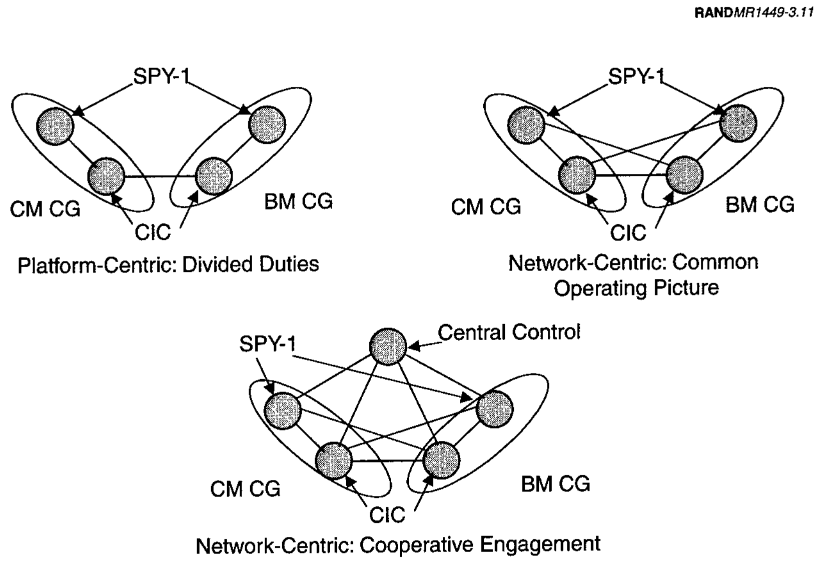

RANDMR1449-3.11
SPY-1
CM CG
BM CG
CIC
Platform-Centric: Divided Duties
SPY-1
CM CG
BM CG
CIC
Network-Centric: Common Operating Picture
SPY-1
Central Control
CM CG
BM CG
CIC
Network-Centric: Cooperative Engagement

Figure 3.11—Missile Defense Operating Procedures

A Reliability Model

In each of the three diagrams in Figure 3.11, each ship is depicted as comprising two nodes: one representing the CIC and the other representing the SPY-1 radar. "Collaboration" between the two consists of passing signals to the radar screen in the CIC and receiving signals from the CIC to adjust the radar's regard. The results of collaboration here are shared information about where enemy missiles are located from the radar and where to look next from the CIC.[29] In the two network-centric cases, the SPY-1 radars are connected to the CICs in both ships. In these cases, the additional information made available by this dual connection is considered a form of positive collaboration and thus increases the reliability of the assessment of

[29] The Office of the Secretary of Defense's Information Superiority Metrics Working Group (ISMWG) defines collaboration to be a process in which two or more people actively share information while working together toward a common goal. See, for example, Alberts et al. (2001, pp. 27–28).

the enemy attack distribution. This is predicated, of course, on the assumption that the information exchanged is of high quality. Finally, in the cooperative engagement case, all shipboard nodes are connected to the central control facility, thereby increasing the opportunity for positive collaboration.

Statistical reliability appears to be an appropriate model for assessing the effects of collaboration. First, we let $c_{ij}(t) \in [0,1]$ represent the effects of collaboration between two nodes i and j, where t is the time required to complete the collaboration. The problem is to examine the nature of the functional, $c_{ij}(t)$, for each collaborative pair and for the entire network. The general form of $c_{ij}(t)$ is:

$$c_{ij}(t) = 1 - e^{-\int_0^t r(s)ds},$$

where $r(s)$ is called the failure rate function and, in this case, is dependent on the nature of the collaboration.[30] Note that for $t = 0$, $c_{ij}(t) = 0$.[31] That is, with no time to collaborate, it is impossible to share any information. With more time to collaborate, we would expect to experience increasing amounts of shared information. To the extent that that is desirable, more time to collaborate leads to improved benefits from that collaboration.

Note that $c_{ij}(t)$ can be viewed as a cumulative probability. If t is a random variable representing the time required for a successful collaboration, then $c_{ij}(t_0) = P(t \leq t_0)$.

As an example, suppose we have a complete network consisting of three nodes—1, 2, and 3. The three nodes therefore generate three collaborative connections, 1-2, 1-3, and 2-3. Suppose that the collaboration probabilities for these three pairs are determined by the following failure rates: $r_{12}(s) = 1$, $r_{23}(s) = 2$, and $r_{13}(s) = 3$. From this, we discover the following collaboration probability functions:

[30] We used t previously to represent the length of a time period. Its current use is quite different.

[31] There are several good texts on reliability engineering. See Ayyub and McCuen (1997) and Pecht (1995), for example.

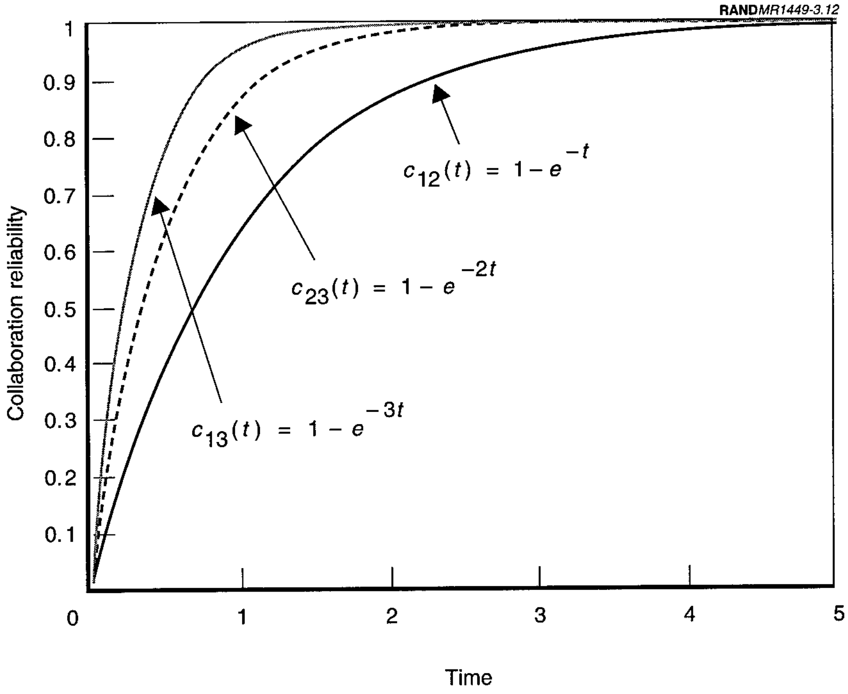


Figure 3.12—Collaboration Reliability Curves

$c_{12}(t)=1-e^{-t}$, $c_{23}(t)=1-e^{-2t}$, and $c_{13}(t)=1-e^{-3t}$. Figure 3.12 depicts varying collaboration probabilities for these three pairs.

Note that the time at which successful collaboration between two nodes occurs depends on the form of its failure rate function, $r(s)$. In this case, a constant was selected because we can model earlier successful collaboration by simply increasing the constant value. In general, we select a form:

$$c_{ij}(t)=1-e^{-\theta t} \text{ for } t \geq 0.$$

The next step is to combine the collaboration effects before assessing its effect on knowledge and subsequently the success of the defensive missions. Before we do this, however, we take advantage of the fact that $c_{ij}(t)$ is a cumulative probability and calculate its density function:

$$f_{ij}(t)=\frac{dc_{ij}(t)}{dt}=\theta e^{-\theta t}.$$

Applying this to the three collaboration estimates we get:

$$f_{12}(t)=e^{-t}$$
$$f_{23}(t)=2e^{-2t}$$
$$f_{23}(t)=3e^{-3t}.$$

These are exponential distributions with $1/\theta$ being the mean time available for nodes *i* and *j* to collaborate with a variance of $(1/\theta)^2$.

The entropy calculation for the exponential distribution with parameter θ is:

$$H(t)=-\int_{t=0}^{\infty}\ln[\theta e^{-\theta t}]\theta e^{-\theta t}dt=1+\ln\left(\frac{1}{\theta}\right)=\ln\left(\frac{e}{\theta}\right).$$

Note that entropy varies with the variance of the distribution as should be expected. As $1/\theta$ increases (θ decreases), $H(t)=\ln(e/\theta)$ also increases. Note also that entropy is unbounded for this distribution.[32]

We can use the entropy function to develop a measure of knowledge by assessing the "certainty" in the density function. This requires an approximate upper bound to be assigned to $H(t)$, the equivalent to assigning a maximum expected time to complete a collaboration. If we let $(1/\theta)_{\max}=\theta_{\min}$ represent the maximum expected time, then a measure of certainty or knowledge can be written as:

[32] This is true for all continuous distributions.

$$K(t) = \ln\left(\frac{e}{\theta_{\min}}\right) - \ln\left(\frac{e}{\theta}\right) = \ln\left(\frac{\theta}{\theta_{\min}}\right).^{33}$$

Note that this quantity is dimensionless and therefore can be used directly to influence combat MOEs. It is desirable, however, for the measure of knowledge to be normalized. This can be accomplished by noting that when $\theta = \theta_{\min}$, $K(t) = \ln(1) = 0$ and when $\theta / \theta_{\min} = e$, $K(t) = \ln(e) = 1$. This suggests the following definition for the knowledge gained from the collaboration between nodes *i* and *j*:

$$K_{ij}(t) = \begin{cases} 0 & \text{if } \theta < \theta_{\min} \\ \ln(\theta / \theta_{\min}) & \text{if } \theta_{\min} \le \theta < e\,\theta_{\min} \\ 1 & \text{if } \theta \ge e\,\theta_{\min} \end{cases}.^{34}$$

Note that for small values of θ, the mean and variance are large, thus implying great uncertainty and therefore little knowledge. For large values of θ, the opposite is true and therefore considerable knowledge is gained. $K_{ij}(t)$, therefore, models the positive effects of having more time, on average, to collaborate.

The next step is to develop a total system collaboration factor that accounts for all pairs of collaborating nodes. The goal is to discern how the enemy proposes to distribute the cruise and ballistic missiles over the τ time periods. This means that the knowledge function, $K(\lambda)$, calculated earlier, should be modified by incorporating the effects of collaboration. Although collaboration between nodes in each of the three cases studied can occur simultaneously, it is necessary that all node pairs collaborate. This makes the overall system collaboration model sequential, and, therefore, using an inverse reliability model we get that system collaboration is:[35]

[33] Because the term *K*(*t*) is derivative of information entropy, we extend the convention of using *t* as the functional argument.

[34] For additional information on the use of information entropy as a measure of knowledge, see Perry and Moffat (1997, pp. 965–972).

[35] It is sequential as opposed to parallel. The latter would occur if the system required that collaboration occur between nodes *a* and *b* or nodes *c* and *d*, but not both. We assume that collaboration occurs between all connected nodes.

$$c_M(t) = 1 - \prod_{[i,j]} c_{ij}(t).$$

Therefore, $c_M(t)$ is large for systems with several collaborating pairs. Using the knowledge factor for each collaborating pair derived from the collaboration function instead of the collaboration function itself, we get:

$$K_M(t) = 1 - \prod_{[i,j]} K_{ij}(t).$$

This assumes that the collaboration effect from each collaborating pair is equal in value. The effects of collaboration then can be represented using a linear model:

$$K_c(\lambda) = K_M(t)[1 - K(\lambda)] + K(\lambda),$$

where $K_c(\lambda)$ is the knowledge about the attack distribution that accounts for collaboration effects. If $K_M(t) \approx 0$, there is little or no collaboration effect. On the other hand, when $K_M(t) \approx 1$, the collaboration effect is "complete" and $K_c(\lambda) \approx 1$.

COMPLEXITY

A well-connected network is necessary for effective command and control, but it is not sufficient. For this reason, we refer to the network as the *potential energy* in a command and control system. The sufficient condition that must be added is the command and control process that operates over the network. This is the *kinetic energy* of the command and control system and to be effective, it must produce quality information and allow for creative command and control arrangements that are reflected in good combat outcomes. It is always possible to misuse a well-connected network and to effectively use one that is not well connected.

As the network in a network-centric operation increases in size, it also increases in complexity. This stems from the actual and potential connections possible. Unless properly managed, this complexity could detract from the mission rather than support it. However, there are cases in which the added richness in connectivity accompanying increases in network size can enhance operations. Hence, complexity as collaboration can have both positive and negative effects.

In this example, collaboration is limited to the two CICs and, in the cooperative engagement case, with the central controlling authority as well. Complexity is generally not a factor in these simple cases. Consequently, we defer the detailed discussion of developing the complexity metric to Chapter Four, where its impact is considerably greater. However, with the addition of other ships in the area participating in the conflict or in the context of other operations in progress affecting the two cruisers attending to missile defense, complexity might become an important factor. For that reason, we include it in the formulation. Unlike the TCT case discussed in the next chapter, we measure the effects of collaboration and complexity on the knowledge function, $K(\lambda)$. Although indirect, the effect of this process on combat outcomes is still measurable.

A Logistics Model

In this work we only examined the degradation in performance stemming from complexity. Although, as will be shown, we can minimize the negative effects through the selection of appropriate parameters, we have not addressed the potential synergies that may derive from a complex network except through collaboration. This remains for future research.

For the divided-duties and shared COP cases, there are four nodes with a maximum of six connections, and, for the cooperative engagement case, there are five nodes with a maximum of 10 connections. Complexity is a function of the number of connections in a network, and, therefore, we let this be the independent variable in calculating its effects. We let C_v represent the total number of network connections for each of the three cases: $v = 1$, divided duties, $v = 2$, shared COP, and $v = 3$, cooperative engagement. Consequently, from Figure 3.11 we have $C_1 = 3$, $C_2 = 5$, and $C_3 = 9$. The general complexity function is:

$$g(C_v)=\frac{e^{a+bC_v}}{1+e^{a+bC_v}},^{36}$$

where a and b determine both the region of minimal impact and the size of the region of rapidly increasing impact. For example, for the three cases described in this analysis, if we let $a = -7$ and $b = 0.9$, we get the curve depicted in Figure 3.13. The values for each case are identified in the figure.[37]

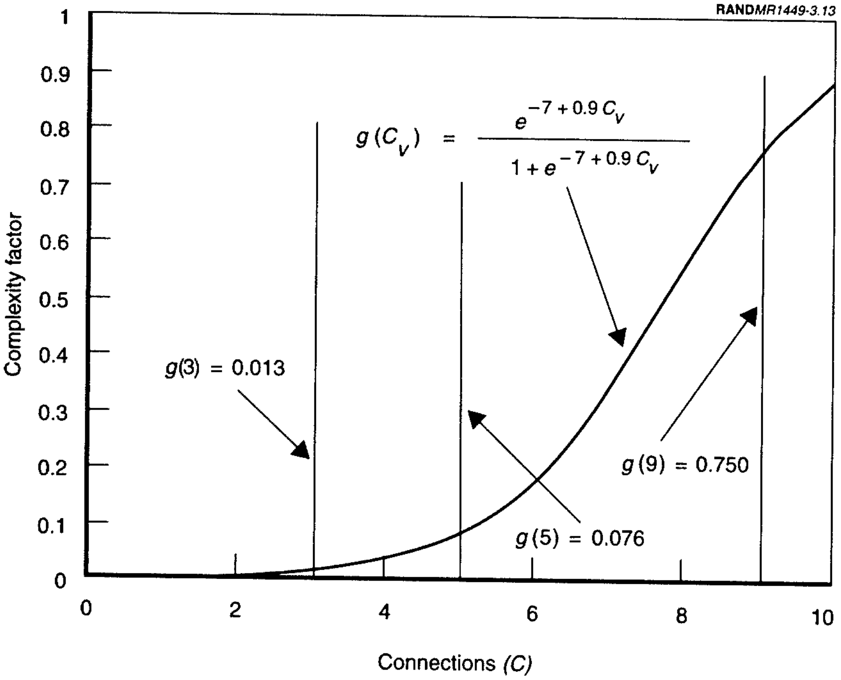


Figure 3.13—Complexity

[36] This curve is sometimes referred to as the *logistics response function* or the *growth curve*. See Neter and Wasserman (1974). See Chapter Four for a more detailed development.

[37] The value, $b = 0.9$, in this example is significantly higher than we might recommend in practice.

We would expect excessive complexity to have a negative effect on our ability to "know" the enemy attack distribution. Therefore, the combined effects of collaboration and complexity on knowledge is:

$$K_{cC_v}(\lambda)=[1-g(C_v)]\{K_M(t)[1-K(\lambda)]+K(\lambda)\}.$$

This is now used to modify the arrival rate estimates at each time period, $\hat{\lambda}_{ci}$ and $\hat{\lambda}_{bi}$. Recall that there are τ arrival time periods, each of which is t minutes in duration. The total number of cruise missiles and ballistic missiles in the enemy's inventory is n_c and n_b, respectively, and the attack horizon is $T = \tau t$ minutes. With no information about the attack distribution, the best estimate is that $\hat{\lambda}_{ci} = n_c / T$ and $\hat{\lambda}_{bi} = n_b / T$. However, with perfect information we have that $\hat{\lambda}_{ci} = \lambda_{ci}$ and $\hat{\lambda}_{bi} = \lambda_{bi}$, the true arrival rates. The following functions incorporate the collaboration and complexity modified knowledge to produce the desired estimated arrival rates:

$$\begin{aligned}\hat{\lambda}_c &= \left(1-K_{cC_v}(\lambda)\right)\frac{n_c}{T}+K_{cC_v}(\lambda)\lambda_c \\ \hat{\lambda}_b &= \left(1-K_{cC_v}(\lambda)\right)\frac{n_b}{T}+K_{cC_v}(\lambda)\lambda_b\end{aligned}.$$

DECISIONS

The implementations of the decisions for the three cases described are addressed next. For all three cases, one of the ships, $A^{(c)}$, searches for cruise missiles and the other, $A^{(b)}$, for ballistic missiles. The decisions center on the allocation policy that best protects both of the cruisers and the critical infrastructure targets.

Decisions are made at the beginning of a period or subinterval depending on the case.

Remaining inventories of Standard missiles on each ship are critical to the decision process. The subinterval consumption rate for these missiles depends on the length of the subinterval, firing rate, shooting policy, and number of ships engaging each missile. The number of Standard missiles (ACM and ABM) fired at each enemy missile is reported in Table 3.1 and repeated for convenience as Table 3.3. The

Table 3.3

Expected Shots Fired

Mode	Expected Shots Fired $(E_f : f = \{c, b\})$
One Ship Engaged	
Shoot	1
Shoot-look-shoot	$2 - p_c$
Shoot-look-salvo 2	$3 - 2p_c$
Two Ships Engaged	
Shoot	2
Shoot-look-shoot	$4 - 4p_c + 2p_c^2$
Shoot-look-salvo 2	$6 - 8p_c + 4p_c^2$

NOTE: In this table, p_c is the single-shot probability that the enemy cruise missile is destroyed. These values are reported in Table 3.1.

number of Standard missiles required to destroy an enemy missile is denoted by the term, E_f, where the subscript denotes either ACMs ($f = c$) or ABMs ($f = b$). E_f is an expected value and is therefore consistent with an expected value analysis, such as this one.

Platform-Centric: Divided Duties

Only the role-switching decision is modeled for this case. The decision is made at the beginning of each interval, and it is based on the remaining inventories of ACMs and ABMs on board each ship and the estimated remaining attack distribution. For a ship to be eligible to assume an ACM or an ABM defense role, it must first have a minimum number of interceptors of the appropriate type in its remaining inventory. Next, the estimated arrival of missiles in this period must be enough to justify the switch.

We let δ_c be the minimum number of ACMs and δ_b be the number of ABMs needed to assume those defense roles, respectively. In addition, we let $I_c^{(c)}$ and $I_b^{(c)}$ represent the remaining inventories of ACMs and ABMs on board $A^{(c)}$. Similarly, $I_c^{(b)}$ and $I_b^{(b)}$ represent the remaining inventories of ACMs and ABMs on board $A^{(b)}$. Inventories of both missile types on board both ships are expected to be reduced by E_f per incoming missile of type *f* as the attack proceeds. The following rules then apply:

1. **When to Switch Roles:** The need to switch roles is based on remaining inventories of Standard missiles on either of the defending cruisers. Consumption of ACMs on the ship designated to defend against cruise missiles and consumption of the ABM inventories on the ship designated to defend against ballistic missiles are factors. A need to switch occurs therefore when either $I_c^{(c)} < \delta_c$ on $A^{(c)}$ or $I_b^{(b)} < \delta_b$ on $A^{(b)}$ or both.
2. **Designated Ballistic Missile Ship,** $A^{(b)}$**:** If a need to switch has been established (rule 1. above), and if the number of ACMs on board exceeds the threshold ($I_c^{(b)} > \delta_c$), and if the inventory of ACMs exceeds the estimated number of cruise missiles arriving in the next interval ($I_c^{(b)} > t\hat{\lambda}_{ci}E_c$), then the ballistic missile ship will assume a cruise missile defense role.[38]
3. **Designated Cruise Missile Ship,** $A^{(c)}$**:** If a need to switch has been established (rule 1. above), and if the number of ABMs on board exceeds the threshold ($I_b^{(c)} > \delta_b$), and if the inventory of ABM missiles exceeds the estimated number of ballistic missiles arriving in the next interval ($I_b^{(c)} > t\hat{\lambda}_{bi}E_b$), then the cruise missile ship will assume a ballistic missile defense role.

Network-Centric: Shared COP

In this configuration, both ships perform ACM and ABM roles. Without coordination of fires, both ships act independently—but with shared information. Each ship engages the targets it feels it can best intercept. Consequently, it is possible that both ships respond to a given enemy cruise or ballistic missile. It is also possible that both ships decide not to respond to a given threat. Several factors combine to determine how often either of these cases will occur. However, we do not treat them explicitly here. Instead, we assume that the fraction of enemy missiles that will be attacked by both ships is given by a constant, γ (we allow γ to vary parametrically).

[38] Note that $t\hat{\lambda}_{ci} = \sum_{j=1}^{s} \frac{t}{s}\hat{\lambda}_{cj}$ where *s* is the number of subintervals within an interval.

In this case, decisions are made at the beginning of each subinterval. The added fidelity is needed to adequately assess the effects of the decisions taken.

The decision to engage an enemy missile is based primarily on the relative geometry (including positions and heading) of the ship and the enemy missile. However, in addition to the relative geometry, consideration is also given to remaining inventories of missiles and the anticipated attack arrival rate for the next subinterval.

In general, it is desirable to engage a threat missile as early as possible. This means that, unconstrained, each ship desires to attack incoming missiles in the order of their proximity to their own ship. The constraints on this behavior is the need to husband inventories. The better each ship is able to anticipate what comes next, the better it can deal with the present threat.

The following decision rule takes location, inventories, and estimates of the future attack distribution into consideration. We focus on the cruise missile threat because this is critical to the survivability of the two defending ships. The same analysis is applied to ballistic missiles.

- **Location:** Although the representations in this analysis do not include relative geometry, we can infer location through the fraction of enemy missiles directed at each of the cruisers (α for $A^{(c)}$and $1 - \alpha$ for $A^{(b)}$). The assumption is that if an enemy cruise missile is directed against either ship, it is likely that that ship will decide it is in the best position to engage it. However, γ percent of the total missile arrivals have an expected impact point that threatens both ships—i.e., in γ percent of the cases, both ships feel that they are the impact point. For these arrivals, decisions are based on both ships attempting to intercept. The enemy intent is to aim α percent of the cruise missiles at $A^{(c)}$ and $1 - \alpha$ percent of the cruise missiles at $A^{(b)}$. The ship $A^{(c)}$ perceives that $\alpha - \alpha\gamma + \gamma$ percent of the arrivals are aimed toward it, and $A^{(b)}$ perceives that $(1 - \alpha)(1 - \gamma) + \gamma$ percent of the arrivals are aimed toward it. An individual ship's decisions are based on this expected arrival allocation.

- **Inventories:** As in all cases, inventories are constraining. If the cruise missile attack in the current subinterval, *j*,

  $$\frac{t}{s}\lambda_{cj} \text{ enemy missiles}$$

  absorbs the entire inventory of ACM ($I_c^{(c)}$ or $I_c^{(b)}$) weapons, then nothing will be left to defend against subsequent attacks.[39] Consequently, current inventories of ACM weapons must be weighed against the current attack and estimates of future attacks:

  $$F_c = \sum\nolimits_{i=j+1}^{s\tau} \frac{t}{s}\hat{\lambda}_{ci}.$$

  For ballistic missile attacks, a similar estimate of future attacks is:

  $$F_b = \sum\nolimits_{i=j+1}^{s\tau} \frac{t}{s}\hat{\lambda}_{bi}.$$

- **Future attack distribution estimate:** The nature of future cruise missile attacks against the two cruisers affects the decision to engage current threats. The anticipation of a more intense attack materializing in the future forces both ships to husband their ACM assets. The decision would be to let the CIWS take care of incoming missiles more likely to hit their targets. We use the parameter, $0 \le w \le 1$, to indicate how much weight we should assign to the future attack in our allocation decision.

The decision rule for $A^{(c)}$ based on these three considerations therefore is to engage a maximum of $d_f^{(c)}$ enemy missiles of type $f\,(f = \{c, b\})$, where $d_f^{(c)}$ is defined as follows:

[39] Note that there are $s\tau$ subintervals in the attack horizon, where s is the number of subintervals in an interval and τ is the number of intervals.

$$d_f^{(c)} = \begin{cases} \beta \frac{t}{s} \hat{\lambda}_{fj} & \text{if } I_f^{(c)} \geq \beta \left(\frac{t}{s} \hat{\lambda}_{fj} + wF_f \right) E_f \\ \beta \frac{\frac{t}{s} \hat{\lambda}_{fj}}{\left(wF_f + \frac{t}{s} \hat{\lambda}_{fj} \right)} & \text{otherwise,} \end{cases}$$

where $\beta = \alpha - \alpha\gamma + \gamma$ when $f = c$ and $\beta = 1$ when $f = b$. Similarly, for ship $A^{(b)}$, we have $\beta = (1-\alpha)(1-\gamma)+\gamma$ when $f = c$ and $\beta = 1$ when $f = b$.

Network-Centric—Cooperative Engagement

In this network configuration as in the shared COP case, the decision to be made is which ship(s) ($A^{(c)}$, $A^{(b)}$, or both) should attempt to intercept incoming cruise missiles in a subinterval and how many missiles each can "safely" engage in a subinterval. The differences between this decision and the shared COP case are as follows: in this case, a central control authority makes the decision based on shared information from both ships, and, in the cooperative engagement case, future attack distributions are considered separately for each subinterval rather than lumped into a single sum of future arrivals (i.e., the computation of F_c). In the COP case, instances occur where both ships attempt to intercept the same cruise missile since defensive fire is not coordinated. In the cooperative engagement case, however, there are also instances where both ships attempt to intercept the same cruise missile. This occurs because the controlling authority has determined that the expected remaining ACM operating life for the remaining Aegis cruisers is longer if both attempt to intercept in the current subinterval. The controlling authority considers the current attack scenario, future expected attacks, and the expected life of each Aegis cruiser that will result under different defensive options. In the cooperative engagement case, the objective of the controlling authority is to use all available information to determine the cruise missile defensive strategy that will keep the ACM capabilities of the remaining Aegis cruiser(s) in operation for the longest period (in terms of subintervals).

It is likely that the enemy will adopt a strategy that focuses on destroying the Aegis cruisers early, thus clearing the way for a concentrated ballistic missile attack. It is also likely that the friendly cruisers will be positioned to provide maximum ballistic missile defense. A longer expected period of ACM operation implies that there is more time to intercept ballistic missile arrivals and to protect the sister ship from arriving cruise missiles. So, the cruise missile defense option that provides the longest expected ACM operating life for the surviving cruisers is then pursued in the current period. As in the shared COP case, our focus during decisionmaking is on defending against cruise missile attack on the defending ships. The ballistic missile defense decisions are similar but of secondary importance. Whatever time and resources are left over in the subinterval will be devoted to the ABM attack mission. Assuming, as usual, that the decision is to be made at the start of subinterval j, we first calculate the number of threatening cruise missiles expected to arrive in each future subinterval

$$\frac{t}{s}\hat{\lambda}_{ci}, (i = j, \ldots, s\tau).$$ [40]

With this and the information assumed available to the decisionmaker, the following decision inputs are used:

- **Inventories:** As in the shared COP case, inventories of ACMs must be carefully allocated to ensure future operation. When a ship's cruise missile inventory is depleted, it may no longer operate in an ACM role. The expected attack size in the current subinterval is

[40] In the absence of any additional information, the expected number arriving in each of the remaining subintervals is

$$\frac{n_c - \sum_{i=1}^{j-1} \frac{t}{s}\lambda_{ci}}{s\tau - j},$$

where the summation on the numerator is the total number of enemy cruise missiles that have already been launched in the preceding $j - 1$ subintervals, n_c is the total number of enemy cruise missiles to be launched, and $s\tau - j$ is the number of subintervals remaining.

$$\frac{t}{s}\hat{\lambda}_{fj},$$

and the remaining inventories for the $A^{(c)}$ and $A^{(b)}$ ships are $I_c^{(c)}$ and $I_c^{(b)}$ ACMs and $I_b^{(c)}$ and $I_b^{(b)}$ ABMs, respectively. For an expected attack distribution, if $A^{(c)}$ is solely responsible for ACM operations, its inventory of ACMs will be depleted in subinterval $v_c^{(c)}$. This occurs when:

$$I_c^{(c)} = \sum_{i=j}^{s\tau} \frac{t}{s}\hat{\lambda}_{ci} E_c^{(c)}.$$

In the formulation of $v_c^{(c)}$, the subscript c indicates the ship is defending against cruise missiles, the superscript, (c), is the ship whose inventory we are assessing ($A^{(c)}$ in this case), and the argument, (c), is the ship defending against the incoming missiles.

We can define similar measures for the ship $A^{(b)}$ and for the case where both ships are performing ACM duties. In the latter case, we assign the ACM duties to the ship with the largest remaining inventory, or when $v(b,c) = \max\{v_c^{(c)}(b,c), v_c^{(b)}(b,c)\}$. Note that the expected number of ACMs fired, ($E_c(c), E_c(b)$, or $E_c(b,c)$) depends on the number of ships performing ACM duties.

- **Expected Survivability:** The survivability of each ship depends on the number of leakers, (L), the single-shot probability that an enemy cruise missile will damage an Aegis cruiser assuming it strikes the cruiser (p_d), and the fraction of damage required to disable the cruiser (p_a). We can then compute the number of leakers required to force the ship out of commission (OOC) and, therefore, render it unable to take on ACM or ABM duties. The number of Red leakers that force a single ship to be OOC is N_L.[41] To take both ships OOC (given that α percent of the cruise missiles are aimed at $A^{(c)}$ and $1 - \alpha$ percent are aimed at $A^{(b)}$), a total of

[41] The formula for the number of leakers required to disable an Aegis cruiser is discussed above under the "Terminal Defense Queue" subhead.

$$N_L^{(b,c)} = \frac{N_L}{\min(\alpha, 1-\alpha)}$$

leakers are needed to disable both ships. At the beginning of subinterval *j*, we compute the quantity:

$$M_j(r) = \frac{N_L^{(b,c)} - L_j}{(1-P_K(r))(1-P_{CIWS})},$$

the additional threatening ACMs that must be launched by the enemy in order to force both ships to be taken OOC, where:

1. L_j is the number of leakers up to the beginning of time period *j*.
2. $P_K(r)$ is the effective probability of kill that can be achieved by the ACMs with *r* defending ships given a fixed shooting policy.
3. P_{CIWS} is the kill probability for the CIWS.

Because the probability of kill for their ACMs and CIWS is the same for both ships, $M_j(1)$ is the same for both $A^{(b)}$ and $A^{(c)}$. Also, we know that $M_j(1) \le M_j(2)$. For an expected attack distribution, the period when both ships are OOC, assuming only one performs cruise missile defense and has an adequate inventory and firing rate to attempt intercept of all missiles, is the subinterval, $\kappa(1)$. This occurs if the following equality is satisfied:

$$M_j(1) = \sum_{i=j}^{s\tau} \frac{t}{s}\hat{\lambda}_{ci} ,$$

When both ships defend, then the period when both ships are OOC is the subinterval, $\kappa(2)$, that satisfies

$$M_j(2) = \sum_{i=j}^{s\tau} \frac{t}{s}\hat{\lambda}_{ci} .$$

Given these values at the beginning of period j and the objective of maximizing the duration of ACM operating life, a decision regarding the number of ACM defenders is made. It is assumed that, once assigned to an ACM defense role, the ship will attempt to intercept every incoming cruise missile in the current subinterval without regard to future attacks (future attacks have already been incorporated in the decision). The resulting decision rules are depicted in Table 3.4.

This decision matrix implies that the priority is to extend the ACM operating life of both ships. Where all cruise missile defense possibilities lead to the same expected ACM operating life, both ships are assigned ACM roles to achieve higher kill probabilities. Finally, when it is decided that only one ship should perform ACM defense, the role is assigned to the ship with the largest ACM inventory.

The assignment rules for ballistic missile defense do not account for survivability of the two ships. In this simple assessment, we neither track the relative survivability of the infrastructure targets nor attempt to prioritize them. Therefore, we assume that all infrastructure targets are to be defended equally. We construct the simple

Table 3.4

Ship Assignment Decision Rules for Cruise Missile Defense

Comparison	Assignment
$\min\{\nu(b,c),\kappa(2)\} \geq \min\{\nu_c^{(c)}(c),\kappa(1)\}$ and $\min\{\nu(b,c),\kappa(2)\} \geq \min\{\nu_c^{(b)}(b),\kappa(1)\}$	Assign mission to both ships
$\min\{\nu(b,c),\kappa(2)\} < \min\{\nu_c^{(c)}(c),\kappa(1)\}$ and $\min\{\nu_c^{(b)}(b),\kappa(1)\} < \min\{\nu_c^{(c)}(c),\kappa(1)\}$	Assign mission to $A^{(c)}$
$\min\{\nu(b,c),\kappa(2)\} < \min\{\nu_c^{(b)}(b),\kappa(1)\}$ and $\min\{\nu_c^{(c)}(c),\kappa(1)\} < \min\{\nu_c^{(b)}(b),\kappa(1)\}$	Assign mission to $A^{(b)}$
$\min\{\nu(b,c),\kappa(2)\} < \min\{\nu_c^{(b)}(b),\kappa(1)\}$ and $\min\{\nu(b,c),\kappa(2)\} < \min\{\nu_c^{(c)}(c),\kappa(1)\}$ and $\min\{\nu_c^{(b)}(b),\kappa(1)\} = \min\{\nu_c^{(c)}(c),\kappa(1)\}$	Assign mission to $A^{(c)}$ if $I_c^{(c)} \geq I_c^{(b)}$ or assign mission to $A^{(b)}$ if $I_c^{(c)} < I_c^{(b)}$

decision rule that both ships will attempt to intercept all incoming TBMs as long as they survive and have not depleted their inventory of ABMs.

SUMMING UP

In this chapter, we have linked the effectiveness of the two Aegis cruisers in defending against both the cruise missile and ballistic missile threat to alternative command and control processes and to alternative operational networks. To do this, it was first necessary to establish adequate measures of effectiveness and performance. Next, we developed mathematical models of collaboration and network complexity to assess the performance of the alternative command and control procedures. Finally, these models were used in an allocation decision process that directly influenced the survivability of the cruisers and the infrastructure targets they were defending.

The Measures

In this vignette, the Aegis cruisers are given two missions: defend against cruise missile attacks against themselves and prevent enemy ballistic missiles from destroying key allied infrastructure targets. For both missions, the measure of success or MOE is survivability—that is, *the fraction of the critical infrastructure targets that survive the attack and the "fraction" of the cruisers that survive the attack.*

The defending ships can detect, identify, and track attacking enemy missiles. What they are less able to do is predict how the enemy will distribute these missiles over time. Knowing the attack distribution contributes directly to the allocation of missile interceptors and therefore to the survivability of both the cruisers and the friendly infrastructure targets. A measure of how well the alternative command and control procedures and networks perform (MOP) therefore is *the degree to which the friendly commander "knows" the enemy's attack distribution.*

The Metrics

Network complexity and collaboration are combined to provide an estimate of the number of cruise and ballistic missiles expected to arrive in the next and subsequent time periods. These estimates are then used in the allocation decision rules for each of the three alternative command and control processes and network configurations. The estimates are:

$$\hat{\lambda}_c = \left(1 - K_{cC_v}(\lambda)\right)\frac{n_c}{T} + K_{cC_v}(\lambda)\lambda_c$$

$$\hat{\lambda}_b = \left(1 - K_{cC_v}(\lambda)\right)\frac{n_b}{T} + K_{cC_v}(\lambda)\lambda_b \, .$$

The terms $\hat{\lambda}_c$ and $\hat{\lambda}_b$ are the current estimates of attacking cruise and ballistic missiles respectively. $K_{cC_v}(\lambda)$ represents the knowledge about the attack distribution informed by the complexity of the network and the collaboration that has taken place. The subscript v refers to the case being examined (v = 1: platform-centric, v = 2: COP, and v = 3: cooperative engagement), λ_c and λ_b are the true attack distributions, and n_c and n_b are the attack sizes for cruise and ballistic missiles to be launched over a total of T minutes. The knowledge function is bounded between 0 and 1 with $K_{cC_v}(\lambda) = 1$ representing perfect knowledge. When this occurs, $\hat{\lambda}_{ci} = \lambda_{ci}$ and $\hat{\lambda}_{bi} = \lambda_{bi}$ and when knowledge is poor ($K_{cC_v}(\lambda) = 0$) we have that $\hat{\lambda}_{ci} = n_c / T$ and $\hat{\lambda}_{bi} = n_b / T$. This last case means that our estimate is that the missiles are uniformly distributed over the attack horizon, T. These equations are the measure of performance.

Chapter Four

A TIME-CRITICAL TARGET

A time-critical target (TCT) is one with a limited window of vulnerability or engagement opportunity during which it must be found, located, identified, targeted, and engaged. Perhaps the most familiar TCTs are mobile theater ballistic missile (TBM) launchers, which can "shoot and scoot." In general, they can be detected while they are moving; in their "hides," they are relatively invulnerable. Once the target is detected, a friendly weapon system must engage it before it returns to its hide.

The problem we are addressing in this chapter is that of an enemy submarine leaving port that is expected to submerge shortly. Like a stationary Scud launcher, a surfaced submarine is highly vulnerable. Submerging increases the difficulty of detecting, classifying, localizing, and killing it. For our example, we assume that the enemy submarine is detected as it leaves port and that an aircraft (or an Unmanned Combat Aerial Vehicle—UCAV—in the futuristic case) will use this cueing data (along with any subsequent updating data) as it tries to attack the submarine before it submerges.

We begin with a description of the vignette in the context of the general scenario presented in Chapter Two. Next, we present three alternative operating procedures and command and control structures designed to solve the problem. Finally, we apply measures and metrics of complexity and collaboration to each alternative and assess the impact each has on the ability to destroy the enemy submarine.

INITIATING EVENTS

On D+5 of the conflict, a U.S. *Los Angeles*-class SSN destroys an enemy attack submarine (SS) operating in the SLOCs northeast of the island. The enemy submarine commander was not able to report the attack to his headquarters on the mainland before sinking.

On D+6, a *Virginia*-class SSN begins a previously planned ISR mission off the enemy coast near the destroyed submarine's home port.

Because the enemy is accustomed to irregular communications with its deployed submarines, it does not realize that its submarine has been killed until D+7. On D+8 a Kilo-class SS is ordered to replace the destroyed submarine. Kilo preparation begins the same day and "overhead" images indicate that the Kilo is preparing to go to sea. Its time of departure cannot be determined from the imagery. However, the Commander of the U.S. Joint Task Force (CJTF) is advised of the Kilo's impending departure and, in turn, advises selected units.

A plan is devised to kill the Kilo on the surface as it emerges from the harbor without revealing the ISR submarine. An F/A-18 fighter-attack aircraft will be vectored to the Kilo and will kill it using a Standoff Land-Attack Missile–Extended Response (SLAM-ER) missile.[1] The SLAM-ER will be guided to the area of the Kilo using a combination of the global positioning system (GPS) and an inertial navigation system (INS), and will acquire and kill it using an electro-optical passive seeker. The performance of this weapon depends on the accuracy with which target position is known at launch, with updates generated by the ISR submarine. An F/A-18 is prepared and placed in "Alert 5" status—it can be launched on five minutes' notice. If necessary, the ISR SSN will step in and kill the Kilo even if this means compromising the ISR mission.

[1] The SLAM-ER is a high subsonic sea-skimming missile with the same electro-optical seeker as the AGM-64 Maverick (made famous in Operation Desert Storm). It uses the same cockpit display as the Maverick. It can work through object recognition or through laser designation. In operation, crosshairs are laid over the target the pilot is able to see. The SLAM-ER then guides itself to the designated target. If the target's area of uncertainty (AOU) is excessive, the SLAM-ER electro-optical sensor may be unable to pick it up. In this case, the pilot can guide the SLAM-ER to reattack and try again.

The Kilo leaves port on D+10 under cover of darkness and is detected by the ISR submarine. Seeing the Kilo's position, course, and speed on the surface, the ISR submarine estimates the remaining time until the Kilo submerges.

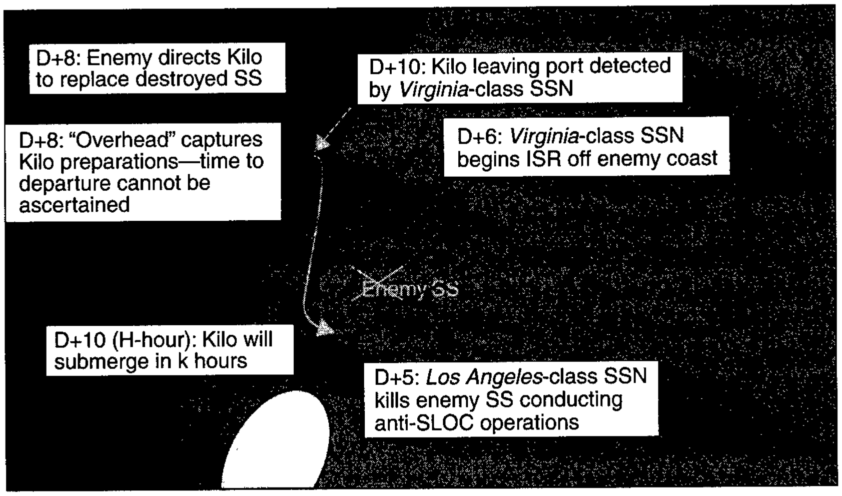
Figure 4.1 summarizes the initial events.

From this point, events are examined from the perspectives of 1980s platform-centric procedures, a current network-centric procedure, and a futuristic network-centric procedure using a UCAV in place of the F/A-18.

MEASURES OF PERFORMANCE AND EFFECTIVENESS

The paramount objective of the U.S. forces is to keep the enemy Kilo from reaching the SLOC north of the island. The JTFC has determined that this can best be accomplished by catching it on the surface and attacking it as early as possible. Nevertheless, the decision he must make is whether to dispatch an F/A-18 armed with a SLAM-ER to attack the Kilo or leave it to the *Virginia*-class SSN even though

RAND*MR1449-4.1*


D+8: Enemy directs Kilo to replace destroyed SS
D+10: Kilo leaving port detected by *Virginia*-class SSN
D+8: "Overhead" captures Kilo preparations—time to departure cannot be ascertained
D+6: *Virginia*-class SSN begins ISR off enemy coast
Enemy SS
D+10 (H-hour): Kilo will submerge in k hours
D+5: *Los Angeles*-class SSN kills enemy SS conducting anti-SLOC operations

NOTE: The circular fans along the enemy coast represent the extent of the enemy's SAM coverage.

Figure 4.1—Initial Events

it is not considered to be the best platform to do this, given that its torpedoes are not optimized for shallow water. In addition, the attack by the SSN would give it away and compromise the ISR mission. The enemy will be unable to infer the source of targeting data relayed to attacking aircraft. The decision therefore hinges on the JTFC's assessment of the time available to him to pursue the airborne option.

The command and control MOP selected for this analysis is Time on Target—i.e., the time available to an attacking aircraft to conduct its attack measured as the time elapsed between its arrival on station and the Kilo's submerging. Since the actual time the submarine will submerge is not known to the CJTF, an earlier arrival time is better than a later one.

The combat MOE is the probability that the aircraft destroys the Kilo given that it arrives on station before the Kilo submerges. The operational impact on the ISR mission is measured in terms of hours of ISR mission lost to supporting an attack against the Kilo, given that the aircraft is unable to engage the target.

ALTERNATIVES

Three alternative operating procedures were developed to analyze this problem. Each makes assumptions about C4ISR systems, connectivity, and weapon systems. The first assumes little connectivity and platform-centric operations. The second assumes a richer network but with only slightly altered processes and equipment. The third assumes a richly connected network with new operating procedures and weapon systems. All three are defined below.

Platform-Centric Operations

Figure 4.2 depicts what is essentially a 1980s platform-centric approach to the submarine detection and acquisition problem. In this operational structure, the ISR SSN reports up the chain of command to the operational commander who then alerts the CVBGs that a threat submarine has left port (steps 2 and 3 in the figure). There is no direct communications between the F/A-18 and the ISR SSN. Note also that the operational commander does not control the ISR SSN, although periodic two-way communications is possible.

RAND*MR1449-4.2*

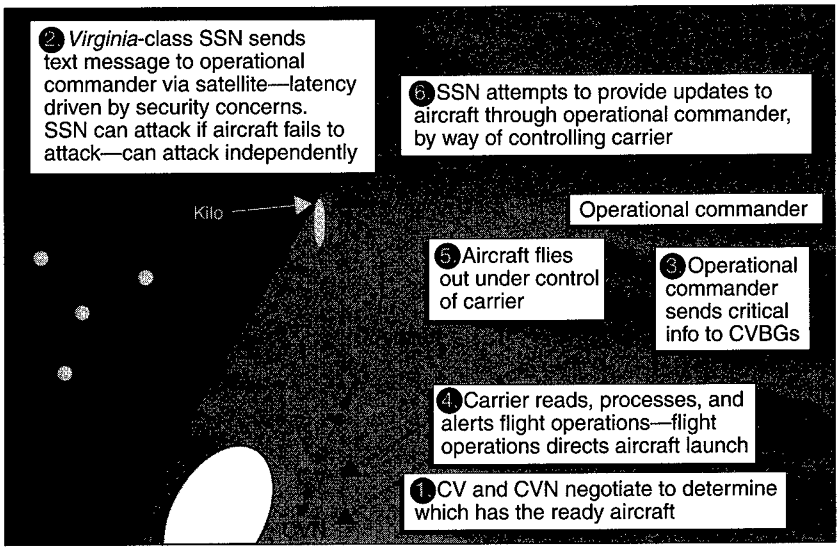

2 *Virginia*-class SSN sends text message to operational commander via satellite—latency driven by security concerns. SSN can attack if aircraft fails to attack—can attack independently
6 SSN attempts to provide updates to aircraft through operational commander, by way of controlling carrier
Kilo
Operational commander
5 Aircraft flies out under control of carrier
3 Operational commander sends critical info to CVBGs
4 Carrier reads, processes, and alerts flight operations—flight operations directs aircraft launch
1 CV and CVN negotiate to determine which has the ready aircraft

Figure 4.2—Platform-Centric Operations

We assume that prior to the operation, the two carriers (one nuclear-powered carrier—CVN—and one conventionally powered carrier—CV) negotiate to determine which will provide the "ready" aircraft, that is, the aircraft that will be on strip alert ready for launch within five minutes (step 1 in the diagram). In this case, the CV is selected.

The CJTF develops the attack plan, using an F/A-18 armed appropriately and placed in "Alert 5" status on the CV (step 4 in the diagram). In this plan, an F/A-18 would fly out and attack the Kilo from outside the SAM envelope (see Figure 4.1) using a SLAM-ER missile (from a range of up to 150 nautical miles). The SLAM-ER will fly out to the estimated position of the Kilo.

The F/A-18 flies out to its launch point under operational control of the carrier, which may determine that the threat to the aircraft is excessive and abort the mission (step 5 in the diagram).

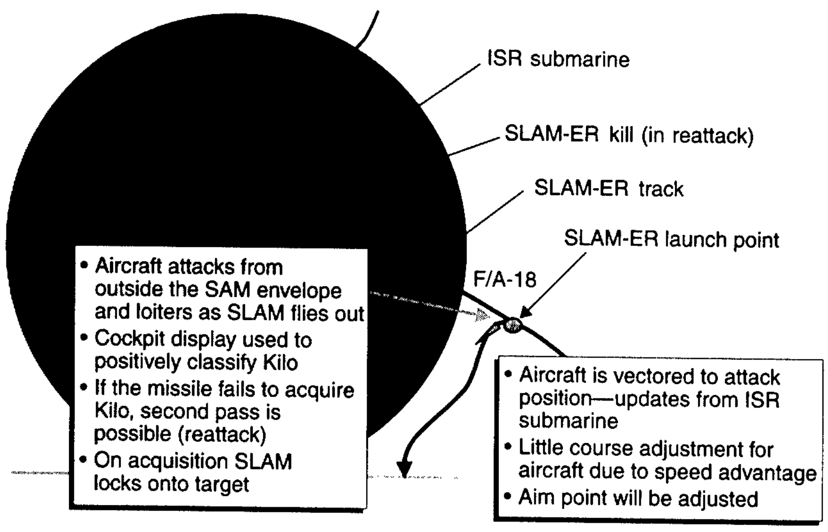
The ISR SSN will continue to provide updates on the Kilo's position, course, and speed, but they will reach the F/A-18 through the operational commander as with the initial message and therefore the updates are likely to be considerably late (step 6 in the diagram).[2]

Figure 4.3 summarizes the details of the SLAM-ER attack and possible reattack.

Command and control in this platform-centric case is split awkwardly between the SSN and air operations on the carrier. The SSN might see an indication that the Kilo was about to submerge and attack it without notifying the other units. In this case, the aircraft would continue on toward a launch point and might go on to an attack based on the last known Kilo position, course, and speed.

Air operations would vector the aircraft and feed it the latest update data. It could determine that the threat level to the aircraft was

RANDMR1449-4.3



- Aircraft attacks from outside the SAM envelope and loiters as SLAM flies out
- Cockpit display used to positively classify Kilo
- If the missile fails to acquire Kilo, second pass is possible (reattack)
- On acquisition SLAM locks onto target

- Aircraft is vectored to attack position—updates from ISR submarine
- Little course adjustment for aircraft due to speed advantage
- Aim point will be adjusted

Figure 4.3—Kilo Attack Operations Using SLAM-ER

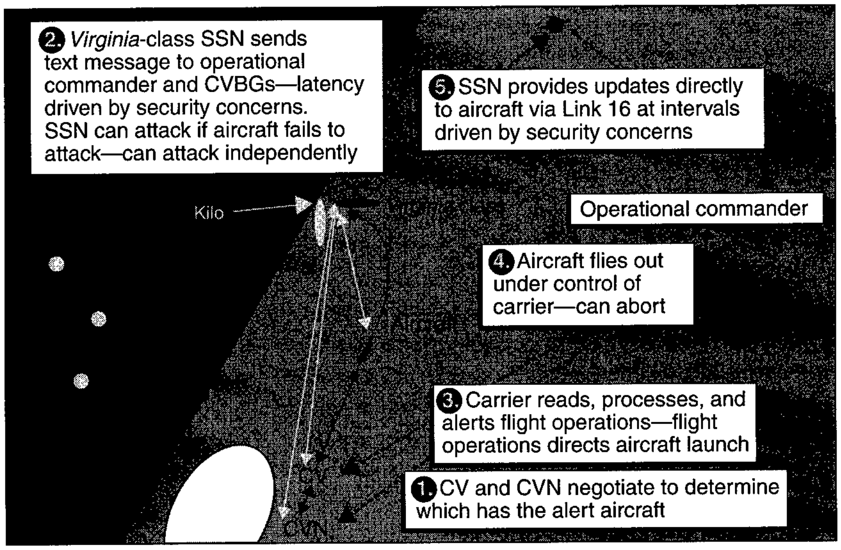
[2] The diagram with shaded and white nodes at the left in Figure 4.2 is a network depiction of the connectivity. The shaded nodes represent entities directly involved in the operations, and the white nodes, although connected, represent facilities or combat entities that either monitor only or provide information. This same depiction is repeated in subsequent diagrams.

becoming excessive and, in that case, abort the mission. This would cause air operations to notify the operational commander that the aircraft mission was aborted and that data would be passed to the ISR submarine. The ISR submarine would ideally attack when the aircraft mission is aborted. Instead, in this vignette, it continues to pass target updates.

NETWORK-CENTRIC OPERATIONS

In this second case, the connectivity among the participants is richer, as depicted in Figure 4.4. The *Virginia*-class ISR submarine has two-way communications (via Link 16) to the carriers. As in the platform-centric case, the ISR submarine also has two-way communications to its operational commander, but these communications can be regarded as "courtesy copies." The fact that the ISR submarine has direct communications to the controlling carrier (and the deploying aircraft) obviates the need to rely on the operational commander to relay messages. Nevertheless, the operational commander monitors communications with the SSN.

RAND*MR1449-4.4*



2. *Virginia*-class SSN sends text message to operational commander and CVBGs—latency driven by security concerns. SSN can attack if aircraft fails to attack—can attack independently

5. SSN provides updates directly to aircraft via Link 16 at intervals driven by security concerns

4. Aircraft flies out under control of carrier—can abort

3. Carrier reads, processes, and alerts flight operations—flight operations directs aircraft launch

1. CV and CVN negotiate to determine which has the alert aircraft

Figure 4.4—Network-Centric Operations

The controlling carrier uses two-way communications with the F/A-18 to control its operation and to confirm threat status updates. The F/A-18 receives periodic target updates directly from the ISR submarine with latency stemming mainly from security considerations (steps 4 and 5 in the figure).

As in Figure 4.3, the F/A-18 will fly outside the SAM coverage envelope to the SLAM-ER launch point and then guide the missile to Kilo acquisition. Relative to the platform-centric process, the area of uncertainty has been reduced to just over one square nautical mile.

The command and control architecture for this version of network-centric operations has the same divisions as the previous platform-centric operation architecture but the consequences of this division are considerably reduced. For example, the ISR submarine may still decide on its own that the Kilo is about to submerge and that the aircraft cannot attack in time and so attack the Kilo itself. However, with communications directly to the carrier, the aircraft can be turned back earlier.

Similarly, if air operations determines that the threat level to the F/A-18 is excessive, the aircraft can be turned back unilaterally. The ISR submarine can be alerted to the situation in its next communication cycle, and therefore it will have more time to attack the Kilo itself.

Future Network-Centric Operations

The Navy's UCAV concept is currently under consideration by the Office of Naval Research (ONR).[3] UCAVs are designed to be launched from a variety of surface combatants in theater and would therefore be an attractive option in this scenario, in that it would relieve the Navy's burden of keeping an F/A-18 (and a catapult) on

[3] The UCAV is designed to be a highly maneuverable, autonomous, Vertical and/or Short Takeoff and Landing (V/STOL) aircraft capable of operating from air-capable ships (other than carriers). It will provide multimission capability including surveillance, target recognition, and air combat to the mother ship. This will involve the development of intelligent control for vision-based navigation, guidance and control, self-optimizing, learning control schemes accepting input from multiple sensory agents and from hierarchies of decisionmaking, and intelligent augmentation for human-centered decisionmaking. See http://robotics.eecs.berkeley.edu/~sastry/onr.ucav/prop/node2.html for more information.

Alert 5 status for days. For the purpose of NCW analysis, we assume that a UCAV will be developed and deployed by the 2010 time frame.[4]

Figure 4.5 depicts the operating environment with UCAVs deployed on a destroyer and a cruiser in the theater of operations.[5] Note the increase in connectivity among the participants in this case from the notional diagram in the lower left of the figure and the geographical depiction.

After the ISR submarine detects the Kilo coming out of port it alerts all potential UCAV launch ships within the limits of its security

RANDMR1449-4.5

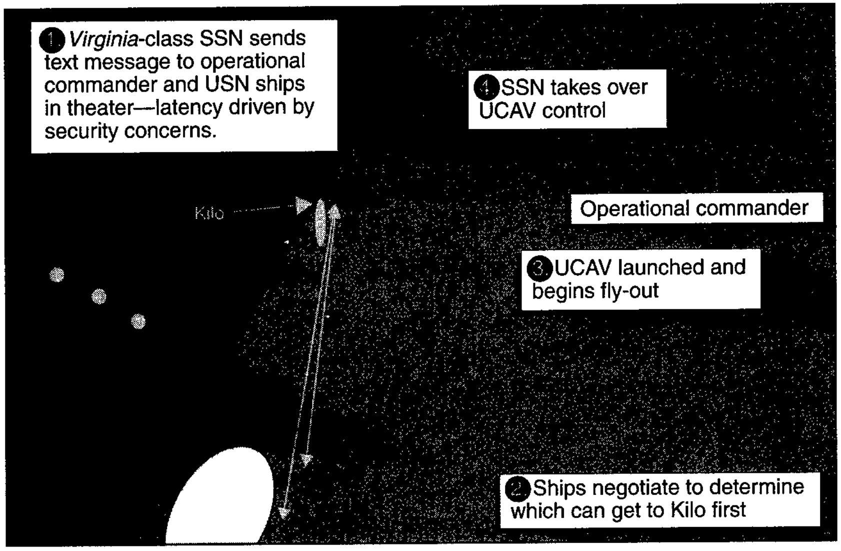

1 *Virginia*-class SSN sends text message to operational commander and USN ships in theater—latency driven by security concerns.
4 SSN takes over UCAV control
Kilo
Operational commander
3 UCAV launched and begins fly-out
2 Ships negotiate to determine which can get to Kilo first

Figure 4.5—Future Network-Centric Operations

[4] At the time this research was conducted, Navy plans were as stated in the text. However, the Navy with Defense Advanced Research Projects Agency (DARPA) support has since moved toward a UCAV platform of aircraft proportions that could only operate from aircraft carriers.

[5] In principle, several other surface combatants might carry the UCAVs. However, for simplicity, we focus on the two platforms only.

concerns (step 1). The ships receiving the message negotiate to determine which can get a UCAV to the Kilo first (step 2). The time to launch a UCAV and UCAV fly-out times would be the determining factors.

In arriving at a decision, the combatants with UCAVs collaborate with each other and with other facilities with information needed to arrive at a best solution. Such issues as who makes the final selection, who determines when sufficient collaboration has occurred, what prior designations have been made, what is the polling frequency, and who determines which combatants with UCAVs are candidates are command and control procedural questions that must be addressed and evaluated analytically.

A UCAV is then launched and begins its fly-out to the Kilo area of uncertainty (AOU) (step 3).

The ISR submarine takes over control of the UCAV, including weapon release (step 4). If the ISR submarine realizes that it must attack the Kilo due to the UCAV's late arrival, the UCAV will be turned back at the next communications cycle. If the submarine determines that the risk of losing the UCAV is becoming excessive (i.e., that UCAV probably will not survive to the launch point), it can conduct the attack and turn back the UCAV itself much more quickly.

The command and control architecture for this case is unsettled. Several options are available, and three of these are listed in Table 4.1. The impact of each option listed in the table is somewhat speculative. However, these (and other possibilities) constitute the basis for conducting exploratory analysis to determine the effects of each on combat outcomes. The results of the analysis of these three options and several variants are reported in Chapter Five.

In addition to the options listed in Table 4.1 are those associated with decentralized command and control. For example, it is possible to establish objective response criteria *a priori* and apply them at execution time. With all ships sharing the same COP, each can determine the ship most suitable to respond without the intervention of a centralized authority in some form of a *bidding* process. True decentralized execution then is based on *negative control* procedures, i.e.,

Table 4.1

Future NCW Command and Control Variants

Option	Process	Impact on Operations
Complete polling at execution time	Poll all potential combatants with UCAVs and select the one that can get to the target quickest	Large cost in collaboration time Fastest fly-out time for UCAV after decision is taken
Periodic selection of a subset of combatants with UCAVs	Poll a select subset of combatants with UCAVs considered to be in the best position to respond. Repeat this process periodically	Less cost in collaboration time Moderate increase in fly-out time for UCAV after decision is taken
Periodic complete polling of combatants with UCAVs	Poll all combatants with UCAVs periodically and designate one as the "duty" launcher	Moderate cost in collaboration time Possibly greatest fly-out time for the UCAV after decision is taken

NOTE: In this context, "polling" is a request from a central authority for information essential to selecting one of the candidate ships with UCAVs to execute the TCT mission. Polling may or may not be automated.

the ship deemed most suitable executes unless vetoed by the JTFC. These procedures are also candidates for further analysis using the measures and metrics proposed below.

LATENCIES

For each of the three cases studied, the time required to perform the required tasks is central to computing the latency MOP necessary to evaluate the effectiveness of TCT operations. Table 4.2 lists the expected (mean) times required to complete the tasks listed along with a reasonable upper bound (the lower bound is, of course, 0). All times are stated in minutes and are converted to hours in the spreadsheet model presented in Chapter Five.

Table 4.2

Expected and Maximum Latencies

	Options					
	Platform-Centric		Network-Centric		Future Network-Centric	
Tasks	Mean	Maximum	Mean	Maximum	Mean	Maximum
ISR SSN alert	15	60	15	60	15	60
SubGroup processing	20	45	20	45	20	45
CV reads, processes, alerts flight operations	10	20	5	10	—	—
CV directs aircraft	2	5	—	—	—	—
Select launch platform	—	—	—	—	2	5
Aircraft preparation and launch	5	10	5	10	—	—
UCAV launch	—	—	—	—	5	10
UCAV fly-out	—	—	—	—	5	10
F/A-18 fly-out	15	30	15	30	—	—
SLAM-ER fly-out	15	20	15	20	15	20
SSN update	15	60	15	60	15	60

NOTE: All times are in minutes.

Platform-Centric Latencies

Communications latencies begin with an alert that the Kilo has left port. Security concerns prevent the ISR SSN from communicating this data immediately. The expected alert latency is estimated to be 15 minutes for the purpose of this study and 60 minutes at most. Note that latencies apply only to the initial alert notice. The ISR SSN will be unable to update the Kilo's position, course, and speed continuously (giving one update on average every 15 minutes and at worst every hour).[6] Data will be current at time of transmission.

Using procedures in effect in the 1980s, the mean time for a submarine group to receive, digest, and retransmit the information from the ISR SSN is 20 minutes with a maximum time of 45 minutes.

[6] These time estimates, and all others in this vignette, are based on discussions with the former commanding officer of an SSN that conducted a similar ISR mission.

At the carrier, the information from the submarine group is read at the Carrier Intelligence Center (CVIC) and extracted to reduce classification level. The information is then conveyed to air operations. The mean time for this manual process is estimated to be 10 minutes with a maximum of 20 minutes.

The update information is then communicated to the F/A-18 with a short delay (estimated at two minutes on average with a maximum of five minutes).

Total latency in *alerting* the carriers is estimated to be 35 minutes on average with a maximum of 105 minutes. Updates to the aircraft are estimated to be just over half an hour on average (32 minutes) with a maximum of 70 minutes. This means that, on average, the F/A-18 will have half-hour-old targeting data at the time of attack. The target area of uncertainty is about 20 square nautical miles for this type of operation.

In terms of operational delays, there will be a delay from the time air operations receives the alert to F/A-18 launch time. This is taken to be five minutes on average and 10 minutes at most (the F/A-18 was kept in Alert 5 status). It must fly out (taken to be 15 minutes on average and 30 minutes at most) to its launch point, with expected SLAM-ER fly-out estimated also at 15 minutes with a maximum time of 20 minutes. It must be launched outside the SAM envelope but within 150 nautical miles of the target.

Several of these latencies will apply in the next two cases as well and therefore they will not be repeated.

Network-Centric Latencies

The time lapse from detecting Kilo egress from port to the alert notice is unchanged. It is still driven by the ISR submarine's security concerns. However, the alert notice and subsequent updates are now delivered directly to the CVIC. Those updates will then be conveyed to air operations within the carrier.

In terms of operational delays, there is no difference from the previous case. It will still take five minutes to launch the Alert 5 aircraft on average, and so on.

Future Network-Centric Latencies

In this case, using the UCAV, the alert messages go out to the submarine group and to the carriers as before. However, a request for a UCAV is sent at the same time to surface combatants with UCAVs in the area of operations. The UCAV ships negotiate to determine which can get a UCAV to the Kilo first, and that ship launches a UCAV. Control of the UCAV is transferred to the ISR submarine.

The distinctive feature of this case is that, whereas an Alert 5 aircraft can be readied days in advance, the decision to designate a surface ship to launch the UCAV is conducted in real time. This is because, as ships move about and ship status changes, the best ship for launching a UCAV can change dynamically.

In this vignette, it is apparent that a UCAV can reach a weapon launch point before an F/A-18 could—it has a significantly shorter flight distance. This is represented by an average five-minute and maximum 10-minute fly-out time for the UCAV as opposed to an average of 15 minutes and a maximum of 30 minutes of fly-out time for the F/A-18. Offsetting this potential advantage is the additional delay imposed while the UCAV ships negotiate to determine the best launch platform (not represented explicitly in Figure 4.5). It is conceivable that, with enough ships in the network, flight time reduction would be more than offset by the additional time required to select a launch platform.

A PROBABILITY MODEL OF KNOWLEDGE

The uncertainties in the TCT problem center on the time required to get ordnance on target. The intermediate times used to collect, process, and disseminate information, all of which are also uncertain, contribute to this time. Because they are uncertain, all are considered to be random variables. They all have the same characteristics in that the likelihood that the task will be completed increases with time. This behavior can best be described with a Gamma distribution, $\Gamma(\alpha,\lambda)$. For this work, we chose the exponential distribution, the special case of the Gamma where $\alpha = 1$. This is made more explicit later. For now, we consider the time, t, required to complete one of the tasks in the TCT problem, where t is a random variable with density function:

$$f(t) = \lambda e^{-\lambda t} \text{ for } t \geq 0.$$

The expected (mean) time required to complete the task is $1/\lambda$ minutes.[7] The uncertainty in this and the other times constituting the overall TCT problem can be taken to reflect a lack of knowledge. Knowing exactly how long each task takes facilitates planning and execution—a lack of knowledge can result in poor planning and mission failure. Consequently, it is important to quantitatively assess the knowledge possessed by the decisionmaker at the time a decision must be taken. As in the missile defense vignette discussed in Chapter Three, we turn to the field of information theory and the concept of *information entropy* or the average information in a probability distribution to characterize knowledge.

Information Entropy

Recall from Chapter Three that information entropy (or Shannon entropy) is a measure of the average amount of information in a probability distribution and is defined as:

$$H(t) = -\int_{t=0}^{\infty} \ln[f(t)] f(t) dt.$$

Applying this to the exponential distribution we get:

$$H(t) = \ln\left(\frac{e}{\lambda}\right).^{8}$$

This suggests the following definition for the knowledge associated with the latency distribution:

$$K(t) = \begin{cases} 0 & \text{if } \lambda < \lambda_{\min} \\ \ln(\lambda / \lambda_{\min}) & \text{if } \lambda_{\min} \leq \lambda < e\lambda_{\min} \\ 1 & \text{if } \lambda_{\min} \geq e\lambda_{\min} \end{cases}.$$

[7] The inverse, λ, is therefore the number of these tasks that can be accomplished in a unit time (minute).

[8] A complete derivation of this term can be found in Chapter Three.

One problem with this formulation is the condition for "perfect" knowledge. This occurs when $K(t) = 1$ or when the expected time to complete a task, $1/\lambda$, is approximately one-third the maximum expected time to complete the task. It may be desirable in some cases to employ more stringent conditions on "perfect" knowledge. This can be accomplished by casting the probability distribution in terms of $M > e$. Although the distribution would not be exactly the form of the exponential with e as the base, it will have a similar form and the condition for "perfect" knowledge will be more stringent. Figure 4.6 illustrates the knowledge function for $\lambda_{min} = 0.5$ completions per hour, or a maximum time of two hours to complete a task.

MOP

We start by assessing the performance of the command and control system in both a platform-centric and network-centric environment.

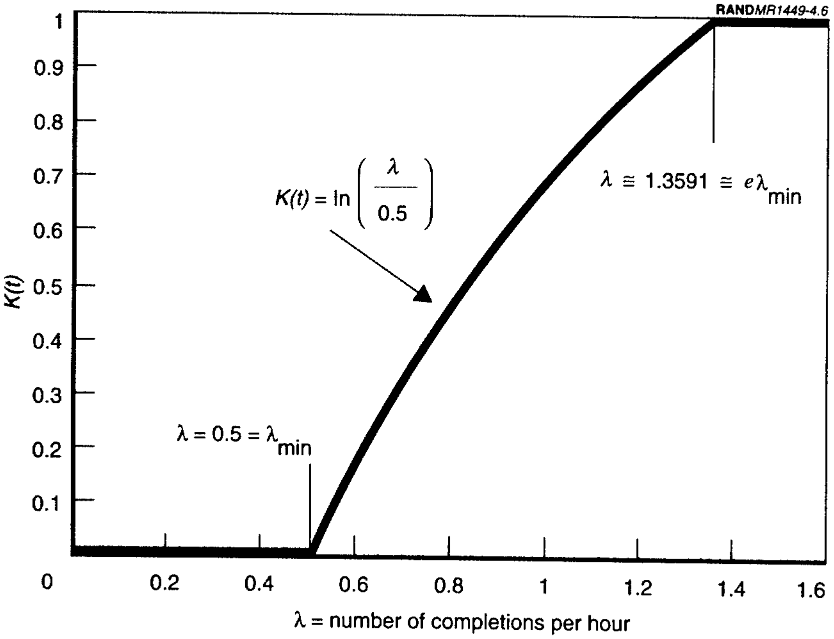


Figure 4.6—The Knowledge Function

The MOP is *time-on-target.* This is defined as the time elapsed from the moment the target becomes vulnerable or can be engaged to the time it is no longer vulnerable or cannot be engaged. In our example, this is the time available for the aircraft (or UCAV) to fly out to the AOU, and detect, target, and kill the enemy submarine before it submerges. Minimizing this accumulated time increases the likelihood that the mission can be accomplished before the submarine submerges and is therefore an appropriate measure of system performance.

Instead of treating the time the Kilo submerges as a random variable and thus introduce additional uncertainty, we instead treat it parametrically. In addition, we assume that no uncertainty exists about the location of the target in that the *Virginia*-class SSN is tracking the Kilo.

Determining time-on-target seems rather simple—i.e., just subtract the latency from onset of target vulnerability to time of engagement from the total time of vulnerability. However, subtleties must be considered.

The Operational Network as a Graph

We begin by describing the command, control, and communications network supporting the operation as an abstraction of a directed graph. A graph, **G**(**X**, **E**), is composed of a set of *nodes*, **X** = $\{x_1, x_2, \ldots, x_n\}$, and a collection of edges, E = $\{e_1, e_2, \ldots, e_m\}$, joining all or some of the nodes. Suppose we have a notional network that consists of *n* nodes with *m* edges. Framing the discussion in terms of a command and control system, we refer to the edges as *connections* and we refer to the graph as the *network*. By "connection," we mean that the "connected" nodes are able to communicate to each other directly. This does not necessarily mean that there is a physical connection between the two. Each connection may have a component that indicates the direction in which the communication of information may flow between nodes. Connections where the communications flow is unidirectional are called *directed connections*. In Figure 4.7, the communication between nodes 6 and 8 is two-way, but the flow of information between nodes 8 and 9 is directional (node 8 may pass information to node 9 but may not receive information directly from node 9). If at least one connection in the network **G**(**X**, **E**) is directed, we refer to the network as a *directed network.* If no connection is directional, the network is *nondirected*. When a network is directed, we refer to the transmitting node as the *initial node* and the receiving node as the *terminal node.*

Of the n nodes in the network, however, only τ are involved in the current operation. The shaded nodes represent those involved in the operation. This is typically the structure of operational networks. Not all potential operational elements are connected and not all are involved in the current operation. For example, Figure 4.7 illustrates a network with 10 nodes but only three are participating in the current operation. There are 15 connections (11 with a single com-

RANDMR1449-4.7

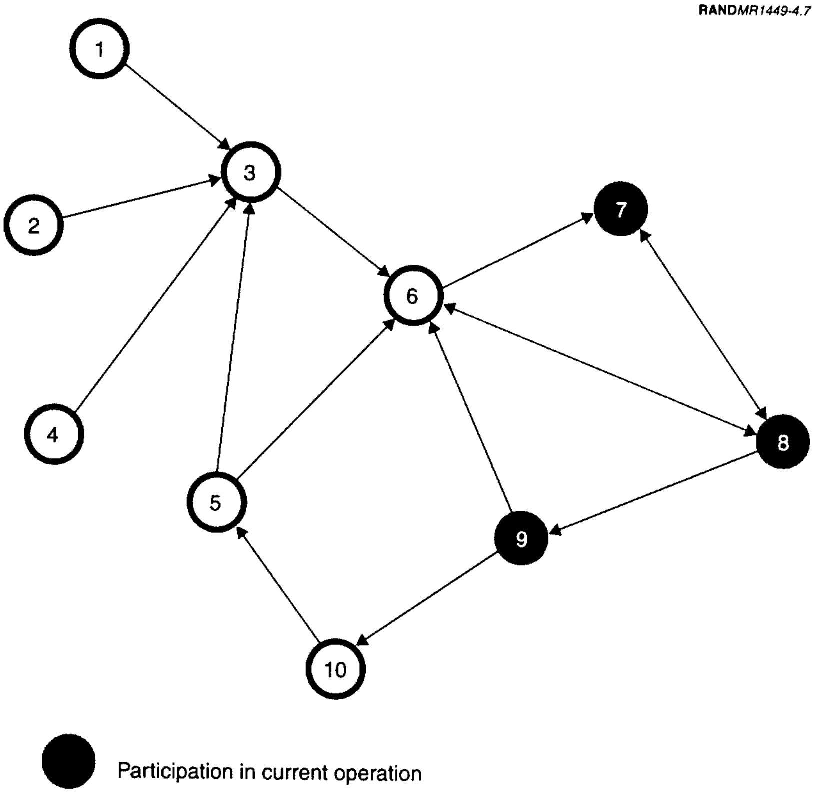


Figure 4.7—Notional Operating Network

munications direction and two that are bi-directional: $11 + (2 \times 2) = 15$) in the total network but only three connections (one one-way and one two-way $= 1 + (1 \times 2) = 3$) between nodes participating in the current operation.

Some interesting relationships arise from this topology however. First, we note that the maximum number of connections in an undirected network with n nodes is:

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

In this case, we have that $m \le [n(n-1)]/2$. In a directed network with n nodes, the maximum number of connections is $n(n-1)$ so that $m \le n(n-1)$. If all the nodes in a graph are connected, the graph is referred to as being *complete*. In the directed network in Figure 4.7, we have a maximum 90 possible connections.

Second, it is important to analyze the role of connected facilities not directly involved in the operation. For example, nodes 6 and 8 are connected to node 7. If node 7 were the CJTF controlling the operation, then 6 and 8 might be information sources (fusion centers on board or remotely located, national intelligence centers, etc.) available to the CJTF. These connections allow the participants to collaborate in arriving at a decision. We expect that collaboration in this case improves the quality (accuracy, timeliness, and completeness) of the decision and is therefore an attribute of the command, control, and communications process that needs to be factored into the overall metric.

The n^2 Phenomena

More important than counting the number of connections of one type or another is the *value* of the connections—i.e., their contribution to combat outcome. If we examine the complete directed graph, we see that there are $n(n - 1) = n^2 - n$ connections. If we assume that all connections contribute to the value of the network, then more connections are desirable. Logically, we conclude that for a very large n, the first term, n^2, dominates and therefore the value of the network increases as the square of the number of nodes in the network increases. This is referred to as *Metcalf's Law,* named for Robert Metcalf, a pioneer in the development of the Ethernet.[9]

The problem with this assessment of a network's value is that it assumes that all interactions are equally "valuable"—that is, that they all contribute an equal positive amount to the value of the network. This is clearly not always the case. The problem of assessing the true value of the network in terms of its contribution to combat outcomes is much more complex.

Too Much Information

Another "law" governing connected networks deals with the propensity of people to utilize available connections to transmit information that may or may not be useful to the recipient. Simply stated, the larger the number of connections in an operational network, the more likely individual nodes will experience "information overload." This is simply a paraphrased Parkinson's Law that "work expands to fill the time available." That is, if a communication channel exists it is likely to be used. This too is compelling—however, like Metcalf's Law it does not apply universally. With proper filtering, extraneous communications can be controlled, especially during critical operations.[10] However, anecdotal evidence seems to confirm that instances of "information overload" occur over undisciplined networks.

Latency

Although not the complete story, the time required to get a weapon on target is an important part of the time-on-target metric. In general, $\tau \leq n$ nodes are involved in the operation. We will refer to these

[9] Robert Metcalf is credited with discovering the Ethernet. He was also founder of the 3Com Corporation of Santa Clara, California, in 1981, the leading producer of Ethernet adapter cards. An interesting discussion of Metcalf and his "law of the telecosm" can be found in Gilder (1993). See also Appendix A to Alberts, Gartska, and Stein (1999).

[10] The actual quote is: "Data expands to fill the space available for storage." Buying more memory encourages the use of more memory-intensive techniques. Those of us who use computers have experienced the wisdom of these words. See, for example, Parkinson (1957).

nodes as the *task force*.[11] Not all need be combat elements; some may be sensors, information processing facilities, etc. The only criterion is that they be directly involved in the mission. The time required for each to perform its assigned tasks contributes directly to latency. Note that we are not concerned about "how well" they perform their task at this point—just how long it takes. It is also possible that the elements of the task force perform their tasks in parallel, sequentially, or some combination of both.

For node *i*, the time, *t*, required to perform all of its tasks in support of the operation is taken to be a random variable with exponential distribution:

$$f(t) = \lambda_i e^{-\lambda_i t},$$

where $1/\lambda_i$ is the mean time to complete all tasks at node *i*. Assuming that all nodes act sequentially, we then get a total *expected* latency of

$$L = \sum_{i=1}^{\tau} \frac{1}{\lambda_i}.$$

Other operating concepts are possible. For example, Figure 4.8 depicts two different concepts, both of which have sequential and parallel processing components. The expected latency for the first concept is:

$$L_1 = \max\left\{\left(\frac{1}{\lambda_6}+\frac{1}{\lambda_7}+\frac{1}{\lambda_8}\right),\left(\frac{1}{\lambda_6}+\frac{1}{\lambda_9}+\frac{1}{\lambda_8}\right),\left(\frac{1}{\lambda_6}+\frac{1}{\lambda_5}+\frac{1}{\lambda_8}\right)\right\}$$

$$L_2 = \max\left\{\left(\frac{1}{\lambda_6}+\frac{1}{\lambda_7}+\frac{1}{\lambda_8}+\frac{1}{\lambda_9}\right),\left(\frac{1}{\lambda_6}+\frac{1}{\lambda_5}+\frac{1}{\lambda_9}\right)\right\}.$$

[11] In graph-theoretic terms, this is called a *subgraph*, G_s(X,E), that contains only a subset of the nodes in X, but contains all of the edges whose initial and terminal nodes are within the subset. Applied to command and control, a subgraph is a subnetwork.

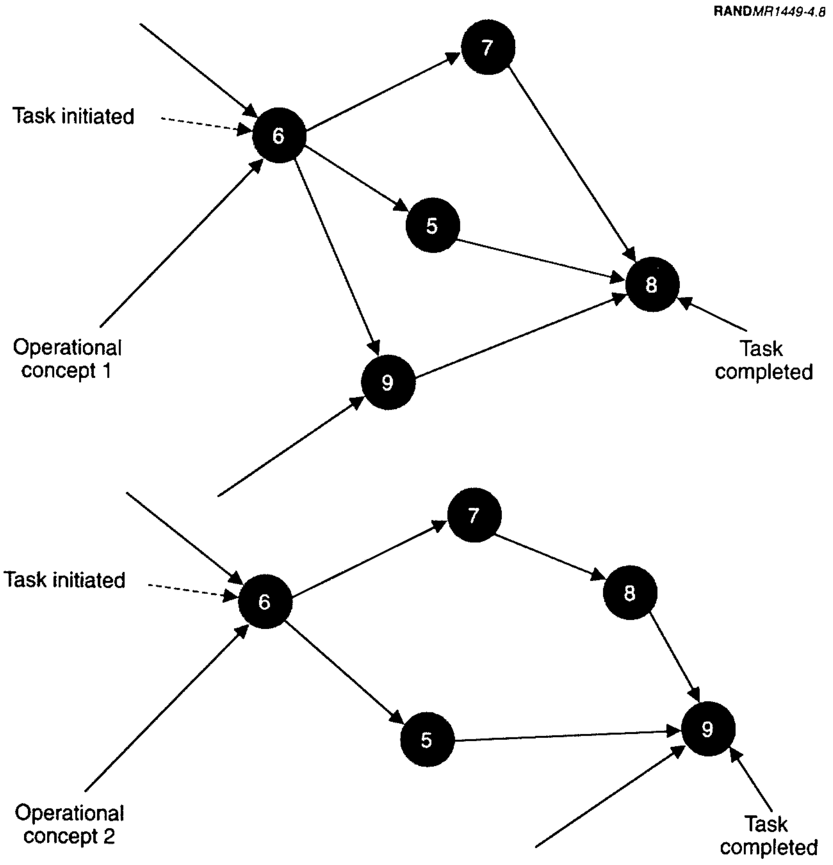


Figure 4.8—Alternative Operating Concepts

Note that only the path nodes are assessed, not the transit time between the nodes. The reason is that we are assessing the delay at the nodes only: The communication time between nodes is taken to be practically instantaneous.

In either case, the *critical path* times constitute the expected latency. If we let $\rho \leq \tau$ represent the number of nodes on the critical path, the expected latency then is:

$$L = \sum_{i=1}^{\tau} \frac{\delta_i}{\lambda_i},$$

where

$$\delta_i = \begin{cases} 1 \text{ if node } i \text{ is on the critical path} \\ 0 \text{ otherwise} \end{cases}, \text{ and } \sum_{i=1}^{\tau} \delta_i = \rho.$$

Also observe that if the effective times required for critical path nodes to complete their tasks are sufficiently reduced, a new critical path may emerge.

Information Quality

In our example, the quality of the information about the location of the enemy submarine is influenced in several ways by the command, control, and communications system. First, the equipment and procedures in place at each of the nodes that contribute to the operation affect the accuracy of the intermediate products produced at that node. For example, the fusion facilities on board the cuing system determine, in part, how well the enemy submarine is tracked. Second, the degree to which the task force is able to collaborate to inform decisions and ensure that a complete picture is at hand increases the confidence that a correct (accurate) decision will be taken. Third, the ability of the task force to access other nodes in the network to complete the operational picture helps ensure nothing is missed. Finally, the amount of training and level of experience of the crews and the length of time they have operated as a team affect the speed with which they are able to accomplish their assigned task—to locate and engage the enemy submarine.

A comprehensive measure of quality therefore would include elements of accuracy, completeness, and timeliness. A validation and calibration process would include adequate representations of each. However, for this work, a suitable measure of quality was taken to be the amount of knowledge available about the expected times required to complete tasks. The quality of the processes and equipment in place at each node, *i*, in the task force is calculated as the knowledge function, and therefore we have a metric, $0 \leq K_i(t) \leq 1$. A value of $K_i(t)$ close to 1.0 implies high quality, whereas one nearer to 0 implies low quality. In addition to the nodes in the task force, we assume that the quality of the products produced by other nodes in the network can also be measured in the same way.

Collaboration's Effect

In Chapter Three, collaboration was defined as a process in which a team of individuals works together to achieve a common goal. It was argued that collaboration enhances the degree of shared awareness in a group focused on solving a specific problem or arriving at an agreed-on decision. In the TCT problem, collaboration consists of sharing information, among the task force members and others in the network, needed to accomplish the mission of locating and engaging the enemy submarine. In general, therefore, collaboration can contribute to the network's ability to support combat operations.

Before we assess the contribution of collaboration to the task of locating and engaging the enemy submarine, we need to expand our discussion of graph theory to include the definition of the *indegree* of a node:

> **Indegree:** The indegree of a node, x_i, in a directed graph is the number of edges that have x_i as their terminal node.[12]

The network graphs in Figures 4.7 and 4.8 are directed graphs. Note that node 6 in Figure 4.7, for example, has indegree 4.

The opportunity for collaboration depends on the number of task force and other nodes each task force node is connected to, or the indegree of the node.

The quality of collaboration as represented by the collective knowledge of the collaboration team has the *effect* of reducing the amount of time required to complete the task (take a decision, order its execution, and take the action required). This is an important point because it may be the source of confusion here and later in the text. By "effectively" reducing the time required, we recognize that although quality collaboration may in fact have no effect on the "actual" time

[12] Taken from Christofides (1975). See also Jackson and Thoro (1990).

required to complete the task, it does provide the opportunity to use the time available more wisely and therefore makes an improvement in the quality of the eventual outcome of the operation more likely. An advantage of this approach is that it can be used to express the quality of collaboration in terms meaningful to operators by translating it into additional time to perform a task or mission.

We should also add here that clearly other factors could be taken into account besides the amount of time required to complete tasks. Each node may contribute something unique to the process, and its ability to do so may be uncertain. This gives rise to the possibility that several random variables, some dependent and others independent, are in play at each node. Combining these uncertainties to form a comprehensive knowledge function is the subject of future research.

For a directed connection, if the quality of the interaction between the terminal task force node, *i*, and any other connected initial node, *j*, is "good," then $K_j(t)$ will be close to 1. This represents the fact that node *j* is able to supply quality information to the executing node. If $K_j(t)$ is large, then $1 - K_j(t) \le 1$ will be small and when multiplied with the actual mean time to complete the task, $1/\lambda_i$, will produce an *effective* latency smaller than the actual latency, $1/\lambda_i$.

If we let d_i be the indegree of the task force node *i*, then the contribution of quality collaboration to node *i*'s operation can be expressed as the product:

$$c_i(t) = \prod_{j=1}^{d_i} \left(1 - K_j(t)\right)^{\omega_j}$$

where

$$\omega_j = \begin{cases} 0.5 \text{ if node } j \text{ is not in the task force} \\ 1.0 \text{ if node } j \text{ is in the task force} \end{cases} .$$

The exponent, ω_j, accounts for the relative importance of the collaboration between two nodes. In this case, in the absence of any experimental data, we use only two levels: important (0.5) and very important (1.0). Perhaps a richer distribution would more accurately reflect the nuances in the effectiveness of the collaboration and its effect on latency, but that remains for further analysis through experimentation.

The total effective latency accounting for collaboration is therefore:

$$L_c = \sum_{i=1}^{\tau} c_i = \sum_{i=1}^{\tau} \prod_{j=1}^{d_i} \left[\left(1 - K_j(t) \right)^{\omega_j} \right] \frac{\delta_i}{\lambda_i}.$$

The *effect* of collaboration is to reduce the total expected time required to complete the mission, and "good" collaboration reduces it further.[13]

Complexity

The concept of network complexity was introduced in Chapter Three, where we deferred the detailed discussion of the subject to this chapter, where its application is easier to assess.

Acting counter to Metcalf's Law, we have noted that in a well-connected network (however large) the possibility always exists that too much information is made available to the task force nodes, resulting in what is generally referred to as "information overload." This can have the opposite effect of collaboration. Instead of effectively cutting the time required to complete tasks, it can prolong the time as staff and commanders sift through the information for what is required. On the other hand, a richly connected network with a well-disciplined command and control system installed can facilitate decentralized decisionmaking and execution and therefore improve the effectiveness of combat operations as well as reduce the time needed to process information.

Network complexity therefore can have both good and bad effects. In this work, we assess the benefits of complexity in terms of collaboration effects and the negative effects of information overload as a factor that increases the time required to perform necessary tasks. It

[13] Note that if one of the quality metric values for a node collaborating with a task force node is 1.0, the time required for the task force node to complete its task is 0. However, the method of calculating the quality metric prevents this from happening.

should be noted, however, that we can mute the negative effects by suitable selection of parameters in the complexity metric.

Complexity then is a function of the total number of connections to the task force nodes, or the total indegree of the operation. Therefore, complexity focuses on the potential misuse of the network, whereas collaboration focuses on the effective use of the network. If we let C represent the total number of connections in the network, then

$$C = \sum_{i=1}^{\tau} \delta_i n_i .$$

For small values of C, the complexity effect is negligible, and for some range it increases rapidly, leveling off at what might be referred to as the information overload point—i.e., when the information arriving from the multiple connections is so great as to practically shut down operations. Although the exact functional relation is not known, a logistic or S-curve relation between C and the complexity factor exhibits the appropriate behavior.[14] If we let $g(C)$ represent the complexity factor, we have:

$$g(C) = \frac{e^{a+bC}}{1+e^{a+bC}} .$$

The parameters a and b determine both the region of minimal impact and the size of the region of rapidly increasing impact. Figure 4.9 illustrates a typical complexity function for the 0 to 90 possible connections for the network depicted in Figure 4.7.[15]

Including complexity in the calculation of expected latency, we get:

$$L_{cC} = \frac{1}{1-g(C)} \sum_{i=1}^{\tau} \prod_{j=1}^{d_i} \left[\left(1 - K_j(t)\right)^{\omega_j} \right] \frac{\delta_i}{\lambda_i} . \qquad (1)$$

[14] The actual relationship should be established through experimentation.

[15] Assuming the logistic curve is the appropriate model for the complexity factor, selecting the coefficients is problematic. They are clearly application-specific and therefore best derived from experimentation. Those depicted in this report are notional.

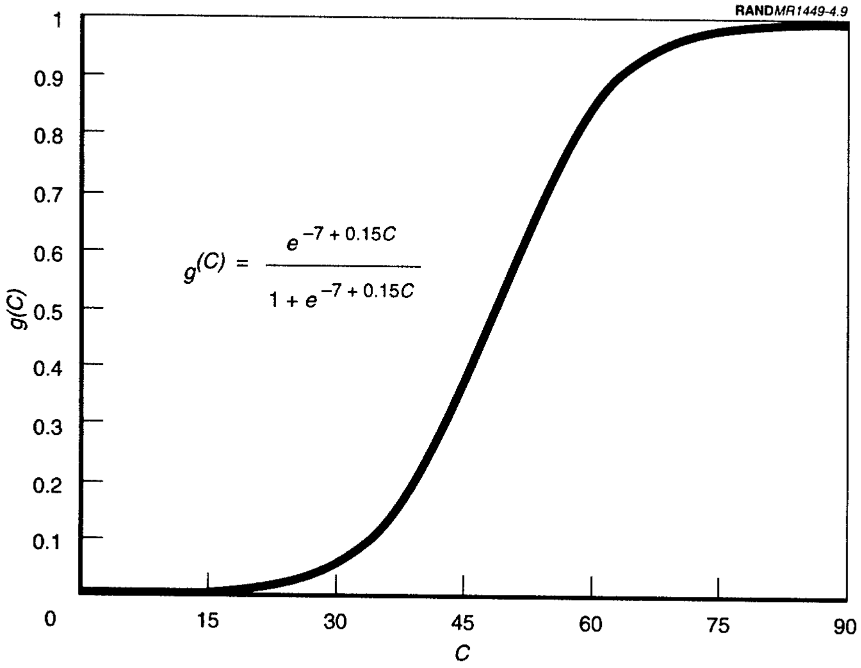


Figure 4.9—Complexity Factor

When the number of connections is low, the complexity effect on latency is minimal. Between about 30 and 60 connections, the complexity effect rises sharply, leveling off to near paralysis at 90.

Effective Expected Latency

Equation (1) reflects the balance between the positive effects of collaboration and the negative effects of complexity. If the effects of complexity are negligible—i.e., there are few connections in the network—and the effects of collaboration are considerable—i.e., the knowledge function for most distributions is high—then it is possible for the expected latency to be much lower than the sum of the critical path latencies. This means that the positive effects of collaboration have compensated for the time required to perform all operational tasks. The converse is also true in a richly connected network where the knowledge functions are rather small. That is, the effective latency can exceed the critical path latency. For this reason, we refer to L_{cC} as the "effective expected latency."

MOE

The measure of TCT effectiveness used here is simply the probability that the target can be attacked during the window of opportunity. For the case of the surfaced threat submarine, it is the probability that the aircraft can detect, classify, and place ordnance on the submarine before it submerges. This probability of detection depends on time on target, the quality (accuracy, timeliness, and frequency) of the location and speed estimates of the enemy submarine, and the characteristics of the attack weapon. For the purpose of illustration, we assume that the aircraft will attack using a missile with an electro-optical system that can detect and classify the threat submarine on the surface. The aircraft is not expected to detect the submarine directly. The pilot will use the cockpit display from the missile to detect and classify the target. The pilot will then lock the missile onto the target. For simplicity, we regard the aircraft as searching the AOU about the target submarine, with the missile used as a remote sensor. We assume a sea-skimming missile with an accordingly short acquisition range, and that once the missile has acquired the submarine it will be killed quickly. In other words, we ignore time of flight over the acquisition range and weapon reliability.

Detection and Target Acquisition

If S is the time elapsed between the moment the submarine leaves port and submerges (in hours), then $T = S - L_{cC}$, where T is the effective search time. If $T \leq 0$, the aircraft fails to engage the target. If $T > 0$, the cumulative probability that the aircraft detects and acquires the target depends on the time it must search the AOU.[16]

If we let $q(T) = 1 - P_d(T)$, where $P_d(T)$ is the probability of detection as a function of search time, then $q(T)$ is the probability that there

[16] For purposes of this analysis, we are concerned with both detection and acquisition. However, for ease of exposition in the sequel, we refer to both as simply "detection."

will be no detections over the same time. For there to be no detection at time $T + dT$, there must be no detection up to time T and there must be no detection in the time interval $T, T + dT$.[17] The instantaneous probability of detection or nondetection depends on search *sweep width* and *search speed* as illustrated in Figure 4.10. It is time invariant. The failure to detect by time T is independent of the failure to detect by $T + dT$. If we let s denote the sweep width in nautical miles, v denote missile speed in knots, and A the AOU in square nautical miles, the probability of detection in the time interval $[T, T + dT]$ is $svdT/A$ and the probability no detection takes place is $1 - svdT/A$. For convenience, we let $\lambda = sv/A$, so that the probability that no detection takes place by time $T + dT$ is $q(T + dT) = q(T)(1 - \lambda dT) = q(T) - q(T)\lambda dT$. Rearranging, we get:

$$\frac{q(T+dT)-q(T)}{dT} = -q(T)\gamma.$$

In the limit as $dT \to 0$, we get:

$$\frac{dq(T)}{dT} = -\gamma q(T).$$

The solution to this differential equation is $q(T) = a + e^{-\gamma T}$ for an arbitrary constant a. Because it is certain that with no time devoted to searching there will be no detection, we have the boundary condition $q(0) = 1$; therefore $a = 0$ and $q(T) = e^{-\gamma T}$. The probability of detection then is:

$$P_d(T) = 1 - e^{-\gamma T}.^{18}$$

As depicted in Figure 4.10, A is a circular region. However, the actual shape of the region depends on what the friendly force knows about the enemy submarine's mission—a priori knowledge. If the Kilo is known to be en route to replace the destroyed submarine, then the

[17] Because these terms are based on T, the "effective" search time, the probabilities are technically "effective" probabilities.

[18] See Koopman (1980).

RANDMR1449-4.10

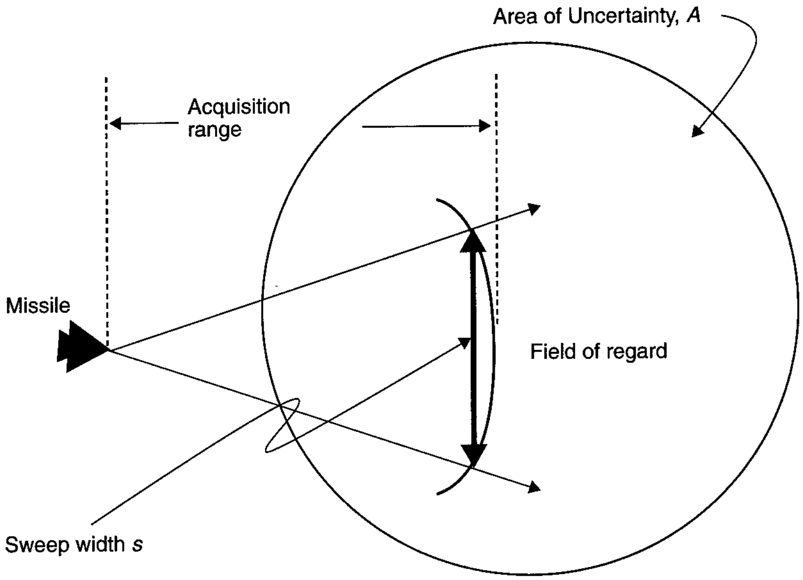


Figure 4.10—Search Operations

friendly commander knows that the full 360° sweep need not be searched in that it is unlikely that the submarine will reverse direction or veer radically off course. The size of the AOU is assumed to increase with the square of the time elapsed since the last Kilo position update. This assumption is consistent with a circular AOU, or a "pie wedge" AOU (reflecting a priori knowledge of heading limits), or an elliptical AOU with fixed eccentricity (reflecting uncertainties in speed and heading). The effect of knowledge in this case is to reduce the size of the AOU by restricting the search to a fraction of the circle coincident with the direction of the submarine.

The size of the AOU depends on the elapsed time, t_u, since the last update and on the speed of the surfaced submarine or:

$$A = \pi\left(\frac{r}{k}\right)^2 = \pi\left(\frac{wt_u}{k}\right)^2,$$

where $0 < 1/\sqrt{k} \leq 1$ is the fraction of the circle that must be searched based on the prior knowledge of the submarine's route of advance. For simplicity, we ignore the possibility that the AOU will grow during the search. Similarly, we ignore the possibility of updating target data during the search. Now, the cumulative detection probability function becomes:

$$P_d(T) = 1 - e^{-\frac{svk^2}{\pi(wt_u)^2}T} .$$

Although the friendly commander has no control over target speed t_u, improved equipment and procedures can greatly affect v, s, and T and good intelligence can affect $\sqrt{k}$.

Figure 4.11 illustrates the increase in detection probability for two cases: when the AOU is 20 square nautical miles and when the AOU is only one square nautical mile. In both cases, the speed of the missile is 450 knots and the sweep width is .25 nautical miles. If we assume that the speed of the target submarine is constant, then the radius of the AOU is dependent solely on the time elapsed since the last update on the target submarine's location. Note the dramatic difference in the results. For the one-square-nautical-mile case, detection probability reaches its maximum within two or three minutes of search, whereas the detection probability for the 20-square-nautical-mile case has still not reached its maximum after 30 minutes of search.

Kill Probability

The probability, $P_d(T)$, is the probability that the target will be detected by time T. This is the cumulative probability distribution for the density function

$$f_d(T) = \gamma e^{-\gamma T} .$$

This function has a mean

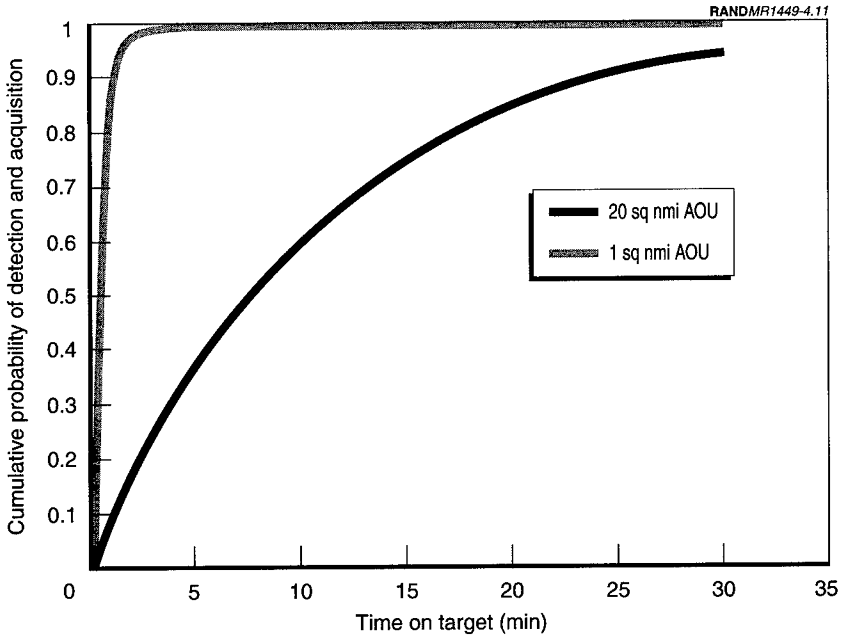


Figure 4.11—AOU Effects on Detection Probability

$$\frac{1}{\gamma}=\frac{\pi(wt_u)^2}{k^2 sv}.$$

This is the expected time required to detect the target. As with times required to collect, process, and disseminate information, a maximum expected time can be determined, and therefore the knowledge resident in the detection time density $f_d(T)$ is assessed as:

$$K(T)=\begin{cases}0 & \text{if } \gamma<\gamma_{\min}\\ \ln(\gamma/\gamma_{\min}) & \text{if } \gamma_{\min}\le\gamma<e\gamma_{\min}\\ 1 & \text{if } \gamma\ge e\gamma_{\min}\end{cases}.$$

This can be used to reflect the quality of the target location estimate by influencing the probability of detection.

In general, if $K(T)$ is large—that is, if the uncertainty concerning the remaining search time is small—we would expect a search more effectively matched to the time available. This also has the effect of reducing the search area. If the amount of reduction is $1 - K(T)$, the effective search area, E_A, becomes:

$$E_A = [1 - K(T)]\left(\frac{wt_u}{k}\right)^2 .$$

Applying this to the detection probability equation, we get the following adjusted detection probability:

$$P_d^*(T) = 1 - e^{-\frac{svk^2}{[1-K(T)]\pi(wt_u)^2}T} .$$

If we let $p_{K|T}^*$ be the knowledge enhanced probability of kill, then in this case where a detection is equivalent to a kill with probability 1.0, we get that $p_{K|T}^* = P_d^*(T)$.

SUMMING UP

In this chapter, we have linked the effectiveness of the SLAM-ER against the enemy Kilo to the speed at which the alternative command and control systems and operational networks are able to get a launch platform on station. To do this, it was first necessary to establish adequate measures of effectiveness and performance. Next, we developed mathematical models of collaboration and network complexity to assess the performance of the alternative command and control procedures.

The Measures

The paramount objective of the U.S. forces in the TCT vignette is to keep the enemy Kilo from reaching the SLOC north of the island. The JTFC has determined that catching it on the surface and attacking it as early as possible can best accomplish this. The decision to dispatch a launch platform (F/A-18 or UCAV) hinges on the JTFC's assessment of the time available to him to accomplish his mission. Consequently, the command and control MOP selected for this analysis is *time on target*—i.e., the time available to an attacking aircraft to conduct its attack measured as the time elapsed between its arriving on station and the Kilo submerging.

The combat MOE is *the probability that the aircraft destroys the Kilo given that it arrives on station before the Kilo submerges.* Because of the accuracy of the SLAM-ER (launched from either the UCAV or the F/A-18), detecting the Kilo is taken to be equivalent to destroying it.

The Metrics

As with the missile defense vignette, network complexity and collaboration combine to affect combat operations. In this case, however, the decision to attack is based on an assessment about the time required to get an attack platform (UCAV or F/A-18) in position to launch a weapon. The expected latency expression is:

$$L_{cC} = \frac{1}{1-g(C)} \sum\nolimits_{i=1}^{\tau} \prod\nolimits_{j=1}^{d_i} [(1-K_j(t))^{\omega_j}] \frac{\delta_i}{\lambda_i},$$

where L_{cC} represents the expected time required to get the attack platform on station, given the effects of collaboration and network complexity. Complexity is included in the expression $1/[1-g(C)]$, and collaboration is a function of the knowledge factor, $K_j(t)$.

The effectiveness of the operation depends on the probability that the enemy submarine will be detected and successfully engaged. This, in turn, depends on the amount of time, $T = S - L_{cC}$, available to search and attack, where S is the time the submarine will submerge. We assume that the SLAM-ER is effective enough that, if detected, a target is assumed to be destroyed with certainty. The MOE therefore is based on the search equation:

$$P_d(T) = 1 - e^{-\gamma T},$$

where $P_d(T)$ is the probability that the submarine will be detected in T minutes. The coefficient γ consists of the geometrical aspects of the problem, such as the AOU, the sensor's field of regard, and the sweep width. In addition, it includes the information update frequency from the ISR SSN and the knowledge gained from external sources.

Chapter Five

EXPLORATORY ANALYSIS TOOL

Changes in MOE values that result from modifying the levels of input variables are best understood by using visualization techniques. By varying the input variables, we can better understand the structure of the data and the complex relationships that exist between the inputs and the MOEs. Such exploratory data analysis (EDA) exercises are, unfortunately, limited to a small number of dimensions. In the presence of high-dimensional data, we are forced to project the data into a smaller-dimensional hyperspace and search for interesting behavior at that level. This projection is most easily achieved by using a single representative value for some subset of inputs—essentially treating them as fixed. Input variables whose range is nonzero are plotted on the available axes with the understanding that the resulting outcomes are conditional on the remaining input variables being fixed. Exploration is then conducted by interactively changing the fixed input values to better understand the relationships between that variable, the input variables shown on the axes, and the resulting MOE.

In this chapter, we suggest a three-step exploratory method for evaluating MOPs and their effects on MOEs. We apply this methodology to the two vignettes discussed in Chapters Three and Four. The data exploration process is dynamic in that inferences can be made only by varying and comparing many different cases. We occasionally discuss examples in which the dynamic EDA yielded a particularly interesting outcome for one of the vignettes. In those cases, the EDA process is paused, the input and output values are captured, and an analytical narrative is included to support the outcome.

STOCHASTIC INPUT VARIABLES

There are three good reasons to create a stochastic simulation to compute measures of effectiveness for combat outcomes in naval operations: the complex interrelationships between variables or between stages of the simulation make it too difficult to explicitly compute; we want each input and the MOE to belong to the finite set of possible real-world values (e.g., we either kill or do not kill a red submarine—we do not kill fractional submarines); and we desire to construct a measure of variability for each MOE.

Suppose we model the single-shot probability of hit (SSPH) of a SLAM-ER against an enemy Kilo according to a Bernoulli distribution with parameter p. That is, p is the probability that a single shot will *hit* the submarine. If we randomly draw n values (simulating n independent shots) from the Bernoulli distribution, the set of possible outcomes will have $n+1$ elements: {0 success, 1 success, ..., n successes}. Each of the $n+1$ numbers of successes is a possible outcome that results from the realization of the binomial distribution. If the random variable X represents the number of successes, then:

$$P(X=x)=\binom{n}{x}p^{x}(1-p)^{n-x} \text{ for } x=0,1,\dots,n$$

with $E(X) = np$, and $\mathrm{Var}(X) = np(1-p)$.

If we used the expected value $E(X) = np$ as the number of successful hits rather than drawing from the binomial distribution, then the set of possible outcomes is not limited to the set of integers {0,1, ..., n}. An expected value calculation may result in an outcome that would be unachievable in a real-world setting (e.g., if np is not an integer).

Suppose SSPH = 0.65 and that five SLAM-ERs are fired (we assume the kth missile is fired even if the Kilo were hit and destroyed by any of the first, second, ..., $(k-1)$th missiles). Then the distribution of hits is depicted in Table 5.1 and illustrated in Figure 5.1.

Based on these results, we can expect that 18.11 percent of all simulations will result in exactly two out of five hits. If our MOE were

Table 5.1

Probability Distribution, Bin (5, 0.65)

x	P(*X* = x)
0	0.0053
1	0.0488
2	0.1811
3	0.3364
4	0.3124
5	0.1160

RANDMR1449-5.1

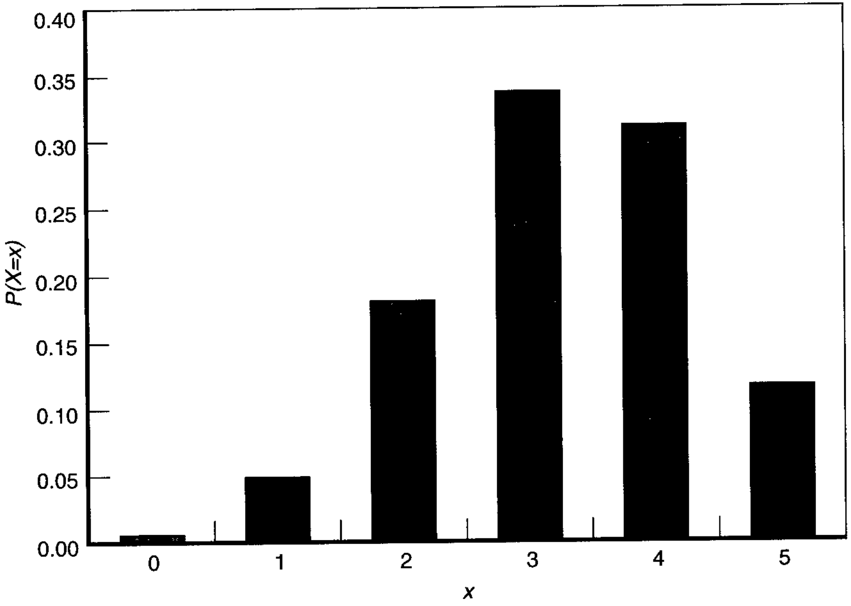


Figure 5.1—Binomial (5, 0.65) Distribution

"fraction of Kilo hits," then we would simulate some damage infliction only for runs where one or more hits resulted (approximately 99.47 percent of the runs).

Essentially, we may consider the simulation-generation process as a transfer function where a vector of random input variables is transformed into an MOE. If the distributions of the input variables are known and the distribution of the function can be computed explicitly, there is no need to simulate outcomes because the theoretical distribution is known. However, as the model becomes more complex, the potential need for simulation becomes greater. For example, if a SLAM-ER is released only when a set of conditions (weather, target detection, etc.) is met, then we need to compute the distribution of the function that transforms all of the other input variables into a decision to shoot or not shoot. In that case, even though the distributions of the set of inputs are known, the sequence of events that determines if the shot is taken is not as straightforward. As the model becomes more complex when more input variables are added, determination of the outcome (in this example, the fraction of Kilos destroyed) increasingly suggests that we simulate the event stochastically.

EXPLORATORY DATA ANALYSIS

Often, we are less concerned with computing the actual value and distribution of the MOE and more interested in MOE sensitivity to changes in the input variables. We are also less interested in the frequency with which each value of an input occurs than we are in seeing how much a change in the value impacts our MOE, given that it does occur. For that reason, we generally define a feasible range over which an input will occur and evaluate the MOE at each value of the input in the range, allowing each discrete value of the input to occur with equal probability. Once we understand the relationship between the input variables and the MOEs, we can then restrict our attention to the range of input values more likely to occur. For example, suppose blue is being subjected to a red tactical ballistic missile (TBM) strike and our MOE is "percentage of airfield damaged." One input variable may be the maximum arrival rate of red TBMs in a time period that may be a Poisson variable with $\lambda = 100$ TBMs. In the EDA, we would evaluate the MOE over a range of arrival rates (e.g., $\lambda = \{50, 75, 100, 125, 150\}$) to understand the relationship between arrival time and the MOE and seek out interesting values that may indicate answers to such questions as, "What is the minimum arrival rate that will result in an expected percentage of airfield damaged of 50 percent?" Given that we understand the relationship between the input and the MOE, we can then increase our focus on the values of λ more likely to occur (perhaps due to intelligence estimates of TBM inventory and firing rate).

To perform the EDA, we suggest selecting a small set of possible values for each input and viewing the MOE over many possible combinations of these. Suppose we have three input variables and one MOE and we have restricted attention to five levels for each input at which we evaluate the MOE. Then, there are $5^3 = 125$ different four-dimensional points for which we can explore the relationship between the input variables and the MOE. Visualization of these various interactions may also help us to identify relationships between independent variables.

Using traditional graphical representations, our visualization capabilities are limited to a small number of dimensions. This implies that, if our system capability is d-dimensional, then we may explore the impact of no more than d–1 inputs on the MOE at one time (the remaining dimension is reserved for the MOE itself). To facilitate EDA over a potentially large number of inputs, we have constructed simple graphical interfaces both for the missile defense vignette in Chapter Three and for the TCT vignette discussed in Chapter Four. The interface allows simultaneous evaluation of three input variables (two statically and one dynamically varied) and one MOE on a single graph. Note also that if there are d input variables, each evaluated at k points, then d^k, the number of possible points at which we need to evaluate the MOE, can grow large very quickly. Our EDA tool provides a way to easily evaluate a large number of input combinations, even when d is moderate (<15) and k is large (>100).

We illustrate the use of this tool for the TCT vignette using a 14-dimensional input set, an MOP ("Effective Time Remaining"), and an MOE ("Kill Probability"). First, we explain how the resulting graphs should be interpreted in the context of expected value and not real-world outcomes of the process being modeled.

EXPECTED VALUE

Earlier, we saw how stochastic simulation allowed complex systems to be modeled in such a way that each simulated input belongs to the set of possible real-world values. In EDA, because we have shifted our focus from the "distribution of outcomes" to the "influence of inputs on outcomes," the need for real-world outcomes can be relaxed. Once that is done, we find it easier to simplify the modeling of the naval operations by employing an expected-value methodology.

Because the exploration of high-dimensional data is difficult, given limited human and computer visualization capabilities, we need a process by which we can use a low-dimensional analysis to understand the structure in high-dimensional data. Our approach is to divide the data into three categories (MOPs/MOEs, design variables, input variables) and then individually evaluate the impact of each "input variable" by cycling through each of them and varying their levels. When we say, "varying the levels," we suggest that the available levels at which the variable may be evaluated is relatively small. Alternatively, we can examine the impact of combinations of input variables and thereby assess the effects of interactions among them. This, however, is rather costly. With just three input variables, each of which has three levels, we get $3^3 = 27$ cases to examine.

The natural question is, "At what level do I set the variables not being considered?" The natural response is, "At the level that we expect it to be." The choice of the term "expected value" requires further discussion because it has two meanings in the context of the EDA.

Expected Value of Distributions

When we simulate, we attempt to represent real-world outcomes as much as possible. In the SLAM-ER SSPK example, we suggested that simulation would result in $n + 1$ possible kill outcomes. Each of the outcomes may occur with some nonzero probability and a fully stochastic simulation will not result in any fractional values for missile kills. However, in the EDA, if the number of shots taken, n_i, and the SSPK, p_j, are considered to be input variables, then each $\{n_i, p_j\}$ pair will have $n_i + 1$ possible outcomes.[1] As part of our dimension reduction, we seek to represent large number of input pairs by generating a single value that represents the weighted average of the

[1] Here, the subscripts i and j are used to indicate the different levels at which we are evaluating the input variables.

distribution of that particular pair of inputs. The summary value that we use is the mean or "expected value." Suppose we look at the SSPK at three points, p_j = {0.60, 0.65, 0.70}, and consider taking between four and six shots, n_i = {4, 5, 6}. From our distribution in Figure 5.1, we know that the {n_i, p_j} pair {5, 0. 65} has six different outcomes and that the expected value is {n_i, p_j} = 5 × 0.65 = 3.25 kills per intercept event. Note that 3.25 kills is not a possible outcome for five attempted Kilo interceptions. Yet, we use 3.25 as an input value in the EDA.

We are not as interested in the actual level of kills as we are in finding the relationship between SSPK and kills, number of shots taken and kills, and the number of shots taken and SSPK (the two input variables {n_i, p_j} are independent in this case, but not in general). By taking expected values, the number of possible outcomes has been reduced from 54 ($5 \times 3 + 6 \times 3 + 7 \times 3$) to nine and the set of triplets {n_i, p_j, MOE$_{ij}$} can be represented as points on a three-dimensional surface plot. Without the expected-value calculation, at least one more dimension would be required to represent the different outcomes that may result from each pair and perhaps another dimension to indicate the frequency at which each of the outcomes will theoretically occur.

As the analysis is extended to include more input variables, the number of possible combinations of input vectors can become staggeringly large. By taking the expected value for each vector, it is easier to summarize the high-dimensional data.

Expected Value of an Input Variable

Expected value has been discussed as a method for summarizing the distribution that results from the interaction of several input parameters in terms of a single value. Expected value may be used in another sense when input parameters are discussed individually. In the SLAM-ER versus Kilo example, 0.65 was used as the value for the SSPK. The choice of 0.65 is based on some information about the SLAM-ER and its historical or simulated killing power against Kilos. However, such questions as, "What if the SLAM-ER performs better than the test data indicate?" or "What if weather degrades the SLAM-ER's visual capability and degrades the SSPK?" may be of interest.

Essentially, 0.65 represents the expected value, and values that we investigate that are different from 0.65 form the basis for exploratory analysis. The expected value is the "base case" and the sensitivity of the MOP/MOE based on small changes in inputs can be evaluated.

RAND EDA TOOL

A complete EDA has three phases:[2]

- **Phase I—an introductory visual exploration:** This allows all possible inputs to occur with equal probability. This phase is used to gain a better understanding of the relationship between input variables and the MOPs/MOEs.
- **Phase II—a focused analysis:** The objective is to restrict the exploration to ranges of input variables more likely to occur.
- **Phase III—a full-scale stochastic simulation:** The simulation does not use the expected value of known distributions but rather randomly draws from them at each simulation replication.

The RAND EDA tool does not provide the capability for the third phase because other simulation systems are already in place. Rather, we choose to focus on the first two phases where important relationships are discovered and the expected impact of policy decisions can be made before undertaking the more costly task of simulation.

TCT VIGNETTE APPLICATION

The data elements for the TCT scenario are organized by the three categories: input variables, design variables, and MOEs as depicted in Table 5.2.

Phase I Analysis

For this vignette we have 14 variables, an MOP, and an MOE. Note that the last four input variables correspond only to the MOE. Because a 16-dimensional space cannot be visualized (11 input vari-

[2] See Bankes (1993).

Table 5.2

Data Elements for TCT Vignette

Input Variables	Design Variables	MOPs/MOEs
Kilo submerge time	Mean CV processing (0–2) hours	Time-on-target
Network complexity penalty	Mean initial SSN report delay (0–2) hours	Kill probability
SubGroup processing delay	Network-centricity (platform-centric, network-centric, futuristic network-centric)	
CVN processing delay		
F/A-18 or UCAV flight/ weapon delivery time		
DDG processing delay		
CG processing delay		
Sweep width		
Missile (SLAM-ER) speed		
Mean time between updates		
Kilo speed		

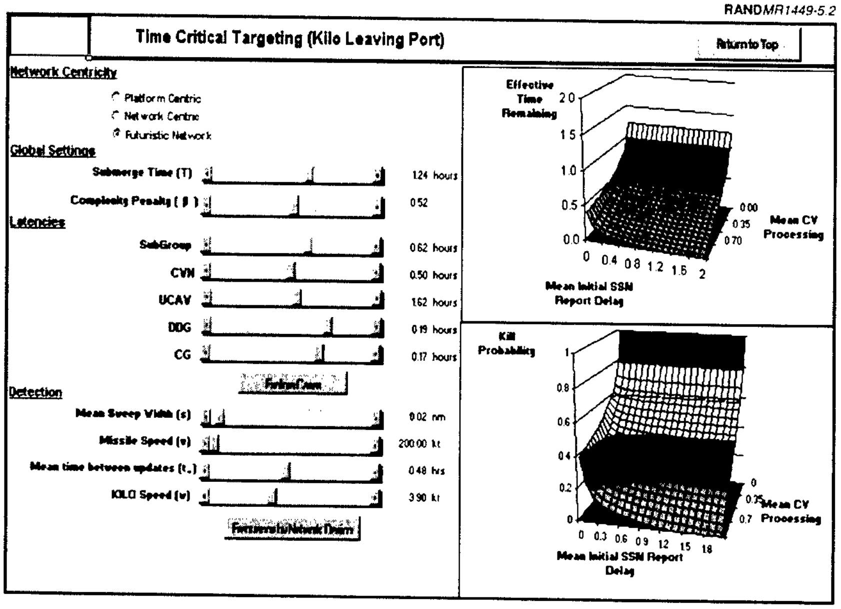
NOTE: Design variables do not change. A range of values for each is plotted provided it is quantitative. If the variable is categorical (such as network-centricity), changes are activated through various controls (slider bars, radio buttons, etc.).

ables + 3 design variables + 2 MOPs/MOEs), the introductory visualization phase of exploratory analysis is accomplished as follows:

- Separate the MOP and the MOE into two separate graphs.
- Plot the quantitative design variables on the x- and y-axes and each MOP/MOE on the z-axis.
- Enable the radio button corresponding to the network topology being studied.
- Individually move the slider bars for the first seven input variables in Table 5.2 to understand the relationships between the input variables, the design variables, and the MOP/MOE.
- Vary the slider bars for the last four input variables to understand the relationship between the MOP and the MOE.

Figure 5.2 is a screen image of the user interface. It depicts how the MOP/MOE response surfaces appear for what is referred to as the

RANDMR1449-5.2



Time Critical Targeting (Kilo Leaving Port)

Network Centricity

○ Platform Centric
○ Network Centric
● Futuristic Network

Global Settings

Submerge Time (T) 1.24 hours
Complexity Penalty (β) 0.52

Latencies

SubGroup 0.62 hours
CVN 0.50 hours
UCAV 1.62 hours
DDG 0.19 hours
CG 0.17 hours

Detection

Mean Sweep Width (s) 0.02 nm
Missile Speed (v) 200.00 kt
Mean time between updates (t_u) 0.48 hrs
KILO Speed (v) 3.90 kt

Figure 5.2—RAND EDA Tool for TCT Analysis (Phase I)

"futuristic network" (Figure 3.9). Some interesting observations can be made:

- As the value of the quantitative design variables increase, the MOP and the MOE become smaller. This is not surprising in that increasing latencies will increase overall latency and therefore reduce the likelihood that the target will be attacked successfully.
- Figure 5.2 shows that the MOP and the MOE are nearly always more sensitive to changes in the Mean CV Processing Time than they are to the Mean Initial SSN Report Delay. Table 5.3 lists a set of approximate partial derivatives,

$$\frac{\partial MOE}{\partial x_i},$$

where x_i = {CV Processing Time, SSN Report Delay}, for the MOE evaluated at nine different points.

Table 5.3

MOE/MOP Sensitivities

Mean CV Processing Time (x_1)	Mean Initial SSN Report Delay (x_2)	$\frac{\partial MOE}{\partial x_1}$	$\frac{\partial MOE}{\partial x_2}$
0.20	0.50	–0.11	–0.54
0.20	1.00	–0.22	–0.35
0.20	1.50	–0.31	–0.29
0.50	0.50	–0.02	–0.58
0.50	1.00	–0.07	–0.39
0.50	1.50	–0.10	–0.32
0.80	0.50	–0.02	–0.59
0.80	1.00	–0.04	–0.40
0.80	1.50	–0.04	–0.34

- Regardless of the detection capabilities, the kill probability is zero when no effective time remains. Although this restates the obvious, it does emphasize the fact that for TCTs, *time* is indeed critical! It is also a good "sanity check."

As the analyst moves through the different combinations that result from dynamic interaction with the slider bars and the network-centricity radio button, the goal of phase I will be accomplished—to gain an understanding of the relationships between input variables, design variables, and the MOP/MOE.

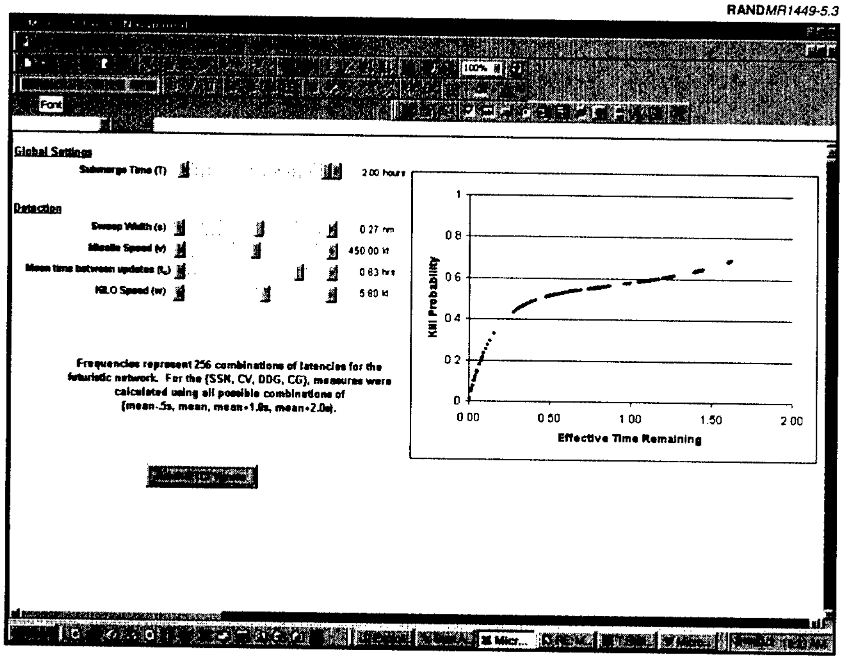
Phase II Analysis

At the outset of phase II of the EDA, the analyst has completely explored the 16-dimensional space by implicitly assuming that each grid point on the response surface for a fixed set of input variables occurs with equal probability. The analytical focus now shifts to examining restricted ranges of a subset of input variables more likely to occur. This is generally accomplished by setting each input variable to its expected value. These are summarized in Table 5.2 above for each of the network configurations.

By setting each input variable to its expected value, a static picture of the response surface is obtained. This represents a best estimate of the MOEs across the range of quantitative design variables and is therefore considered to be the "base case." In phase II, deviations from the "base case" are explored to get an idea of the range of values that may occur in the event that the actual values of the input variables differ from the expected values. In the exploratory tool, this second phase is provided only for the futuristic network-centric case. When this case is enabled via the radio button, the user may then click on the "Explore cases" command button that activates the phase II analysis.

Figure 5.3 depicts the phase II analysis screen. In this example, the expected values of the SubGroup, CV, UCAV, and complexity penalty have been fixed. A subset of the input variables is depicted and can be varied using the slider bars provided. The remaining input/design variables are evaluated at a small set of points: their individual means, one-half standard deviation below their means, one standard deviation above their means, and two standard deviations above their means (see Table 5.4). Since we vary four input variables at four points, there are $4^4 = 256$ different outcomes for each combination of

RANDMR1449-5.3



Global Settings

Submerge Time (T) 2.00 hours

Detection

Sweep Width (s) 0.27 nm

Missile Speed (v) 450.00 kt

Mean time between updates (t_u) 0.83 hrs

KILO Speed (w) 5.60 kt

Frequencies represent 256 combinations of latencies for the futuristic network. For the (SSN, CV, DDG, CG), measures were calculated using all possible combinations of (mean-.5s, mean, mean+1.0s, mean+2.0s).

Figure 5.3—RAND EDA Tool for TCT Analysis (Phase II)

Table 5.4

Mean and Standard Deviation Settings for the Futuristic Network

	Variants			
Input Variable	Mean (1/ λ) in Minutes	1 / 2λ	2 / λ	3 / λ
DDG processing delay	15	7.5	30	45
CG processing delay	10	5	20	30
CVN processing delay	17	8.5	34	51
SSN initial report time	15	7.5	30	45

inputs implied by the position of the four slider bars.[3] Each case generates a value for the MOP and for the MOE. These values are then displayed in graphical form. The chart at the right in Figure 5.3 illustrates the interdependence of the MOP (effective time to attack the enemy submarine) and the MOE (probability of kill) generated from the 256 points.

The reason for evaluating both the MOP and the MOE at a discrete set of points is to assess the worst- and best-case scenarios. For example, from Figure 5.2, we learn that an increase in the CVN processing time has a very large impact on either the MOP or the MOE. So, it may be of interest to assess their values in a "worst-case" situation where the value of the input is two standard deviations above its mean. In this phase, it is no longer assumed that the 2/ λ case will occur with equal probability with the expected-value case (for most distributions). However, it is understood that the 2/ λ may occur with known, nonzero probability.

Once the slider bars are dynamically moved, the plotted points are observed to see if they tend to cluster in certain regions or if they tend to separate for certain values of input variables. Once that relationship is understood, the slider bars may be set at their expected values and focus can now shift to the examination of specific cases. For example, there appears to be two points in Figure 5.3 where both measures are higher than any other points in the 256 cases. In fact, their values can be found by placing the mouse over the point of

[3] Of course, varying more variables or selecting more variants for each will produce more alternatives. Nothing is sacred about four variables and four variants each.

interest—these two yield values of {1.60, 0.683} and {1.61, 0.683}. Below the graph section, the input data values and resulting MOEs are available, and so the analyst may then look up the values that generated the interesting point on the graph.

Analysis of Polling Options

We now apply the process to the polling options for the futuristic network first presented in Table 4.1 and reproduced here as Table 5.5 for convenience.

The research question is, "How should the platform assigned to launch the UCAV be designated?" This is essentially a command and control question that addresses the way the richly connected network is utilized to support combat operations. The three choices offered have implications for the effective time available to attack the Kilo. All three are associated with the times required for collaboration and UCAV fly-out. In Table 5.5, the platform collaboration times and the UCAV fly-out times are listed for all three options.

Polling at execution time: This is the most reliable method in the sense that the combatant who can get a UCAV to the target most

Table 5.5

Future NCW Polling Variants

Option	Process	Impact on Operations
Complete polling at execution time	Poll all potential combatants with UCAVs and select the one that can get to the target quickest	Large cost in collaboration time Fastest fly-out time for UCAV
Periodic selection of a subset of combatants with UCAVs	Poll a select subset of combatants with UCAVs considered to be in the best position to respond. Repeat this process periodically	Less cost in collaboration time Moderate increase in fly-out time
Periodic complete polling of combatants with UCAVs	Poll all combatants with UCAVs periodically and designate one as the "duty" launcher	Moderate cost in collaboration time Possibly greatest fly-out time for the UCAV

quickly is always selected. However, considerable time can be absorbed by collaborating to arrive at an "optimal" selection based time to launch a UCAV (which may depend on readiness) as well as distance to the target.

Polling of a subset at execution time: In this case, a periodically preselected subset of the platforms with the UCAV is polled at execution time. Because the number of platforms polled is reduced, the collaboration time required at execution is not as great. The fact that the preselection is time-consuming has little impact on the delay at execution time. The reliability of the preselected choice in terms of the time required to reach the target is however, reduced. This is because it relies on a best-estimate process and because the data on which a best estimate was developed may not apply at the time of execution. UCAV launch readiness may have deteriorated in the interim, for example. The result is that combined time for UCAV launch and fly-out can be extended.

Periodic complete polling: In this case, the entire set of platforms with the UCAV is polled periodically. The polling takes place prior to the operation, meaning that little time is spent deciding which platform will launch the UCAV at execution time. The reliability of the preselected choice, however, is less reliable than selection at execution time. In this case, the fact that *all* platforms are polled mitigates the deficiency somewhat. The impact on fly-out time for the UCAV is generally greater than the first case.

Analysis of the Three Polling Cases

Table 5.6 lists the mean times associated with the three cases discussed. Note that only the times likely to vary based on the conditions described are listed. The values for all other variables (input and design) are fixed. For each case, there are 441 possible alternatives corresponding to the grid points of the EDA tool shown in Figure 5.2. Although not shown, 21 data points on both the *x*- and *y*-axes thus produce 441 possible points on the *z*-surface. The fly-out time is fixed for each case. Note that the two other times associated with the attack sequence (UCAV launch and SLAM-ER fly-out) are not affected and therefore remain fixed.

Table 5.6

Time Estimates for Polling Variants

Option	DDG Polling	CG Polling	CVN Polling	CV Polling	UCAV Fly-Out
Case I: complete polling at execution time	15	10	17	17	5
Case II: periodic selection from a subset of UCAV platforms	8	7	—	—	20
Case III: periodic complete polling of UCAV platforms	8	7	9	9	10

Figure 5.4 illustrates the analysis tool needed to assess the relative effectiveness of the three cases. Access to this tool is from the screen depicted in Figure 5.2. The button titled "Frequency by Network Design" provides access to the screen depicted in Figure 5.4.

RANDMR1449-5.4

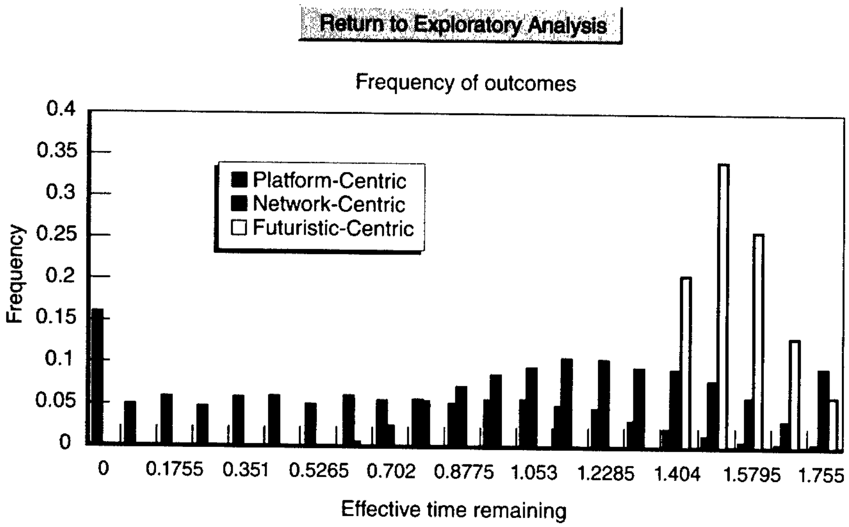


Figure 5.4—Comparing Alternative Network Designs

The graphic depicted in Figure 5.4 is a histogram of the 441 alternatives generated by a single case as described above. All three network configurations are included on a single figure. In this example, we will only be interested in the futuristic network case across the three sets of variable settings in Table 5.5. The x-axis in the figure is the effective expected time available to attack the target (the value *T* described in Chapter Three) and the y-axis is the fraction of the 441 alternatives that resulted in the x-axis times. Therefore, clustering of occurrences to the right of the figure is desirable. Note that in the sample, the platform-centric network is skewed to the left somewhat with only a few occurrences exceeding one hour. The network-centric case fares a bit better with no alternatives below 30 minutes and with the largest concentrations being between 60 and 80 minutes. However, the futuristic network is clearly superior with no alternatives less than 84 minutes.[4]

UCAV Analysis

Figures 5.5 through 5.7 depict the results of setting the five input variables in Table 5.5 to the three values depicted. Only the futuristic network cases in each are relevant to this analysis (the unfilled bars in each figure). Note that the maximum time available to attack the target for any of the cases is 1.755 hours, or approximately 105 minutes. This means that the minimum effective, expected latency is approximately 15 minutes. That is, factoring in all the positive effects of collaboration and the negative effects of complexity, the minimum effective, average time required to get the SLAM-ER to the target area is 15 minutes.

The analysis focuses on the measure of performance only. Because the MOE is directly proportional to the MOP for fixed search parameters, this is adequate. Table 5.7 summarizes the frequencies depicted in each of the cases. If we focus on the maximum effective time available (105 minutes), it is clear that periodic polling (Case III) is superior with 58 percent of the 441 alternatives or approximately 256

[4] These times are all based on a two-hour window. That is, the enemy Kilo will submerge within two hours.

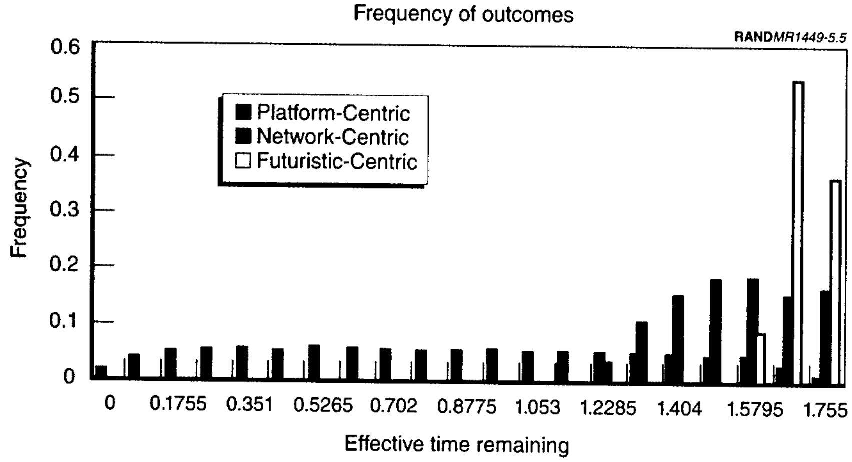


Figure 5.5—Polling All Platforms at Execution Time

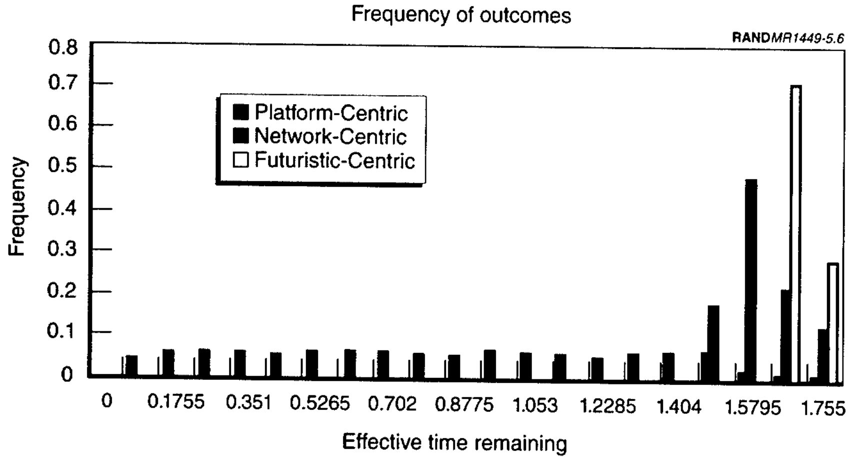


Figure 5.6—Polling a Subset of UCAV Platforms at Execution Time

alternatives allowing for this much search time. If we focus on the 100-minute-time-available case, the periodic selection of a subset of UCAV platforms (Case II) is superior with 71 percent of the 441 alternatives, or approximately 313 alternatives allowing for this much

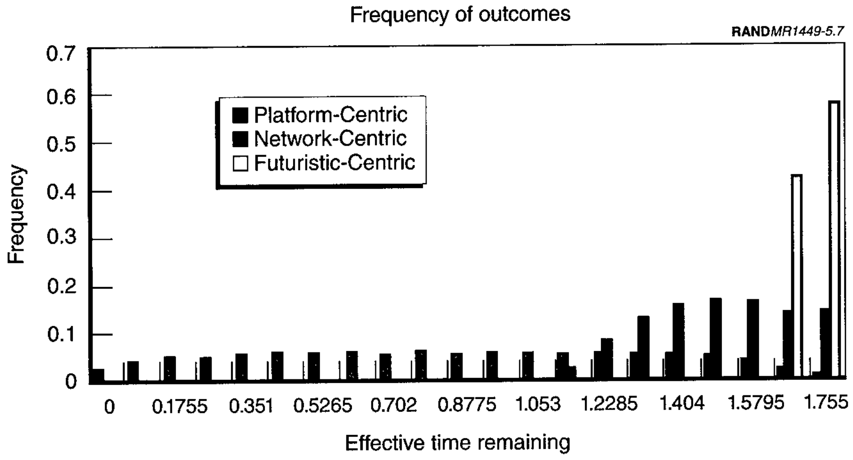


Figure 5.7—Periodic Prepolling of All UCAV Platforms

Table 5.7

Results of Alternative UCAV Platform Selection Processes for the Futuristic Network

	Time Available		
	105 min	100 min	95 min
Case I: Complete polling at execution time	38	53	9
Case II: Periodic selection from a subset of UCAV platforms	29	71	0
Case III: Periodic complete polling of UCAV platforms	58	42	0

NOTE: Entries in the table represent the percentage of the 441 alternatives in each category.

search time. Note that Cases II and III together dominate Case I, polling all platforms at execution time.

The results suggest that Case III is the preferred way to operate. However, as mentioned earlier, this should be the beginning of a more detailed assessment of the alternatives in Case III to determine why 58 percent of the alternatives yielded the 105-minute time available. The analyst may wish to examine the effects of other variables to include those associated with the search equation. Also, it is important that before real analysis is conducted using these concepts, considerable validation and calibration must be accomplished.

MISSILE DEFENSE APPLICATION

We next perform the first phase of the EDA on the missile defense scenario. Phase II of the EDA is not developed here because the alternative network configurations are depicted in the phase I displays.

The data elements for the missile vignette scenario are organized by the three categories: input variables, design variables, and MOEs as depicted in Table 5.7.

Phase I Analysis

For this vignette we have 23 variables and two MOEs. Because a 25-dimensional space cannot be visualized (21 input variables + 2 design variables + 2 MOEs), the introductory visualization phase of exploratory analysis is accomplished as follows:

- Separate the two MOEs into two separate graphs.
- Plot the quantitative design variables on the x-axis and each MOE on the y-axis.
- Split the input variables into the appropriate side (red or blue) and individually move the slider bars for input variables in Table 5.7 to understand the relationships between the input variables, the design variables, and the MOEs. The plotted MOEs are updated simultaneously on the red and blue pages where input variables are set.

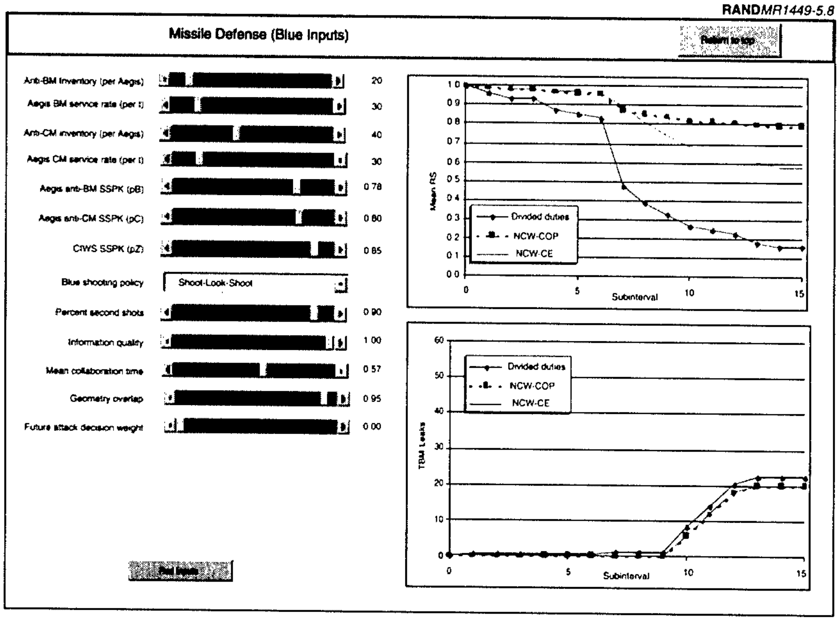
Figures 5.8 and 5.9 are screen images of the user interface. Figure 5.8 depicts blue inputs and Figure 5.9 depicts red inputs. In Figure 5.9, the user is able to use the scroll bars to set the true arrival rate for red cruise missiles and ballistic missiles. In the example, we have an attempted cruise missile saturation where nearly all cruise missiles arrive uniformly in each subinterval of the third interval. Following that, in interval four, a majority of the ballistic missiles are delivered uniformly in each subinterval.

Table 5.8

Data Elements for Missile Defense Vignette

Input Variables	Design Variables	Measures of Effectiveness
Threatening red ballistic missile count	Network-centricity (divided duties, COP, cooperative engagement)	Mean remaining survival
Threatening red ballistic missile arrival distribution	Subinterval length	Cumulative ballistic missile leaks
Threatening red cruise missile count		
Threatening red cruise missile arrival distribution		
Percentage of red cruise missiles aimed at *A(b)*		
Cruise missile single-shot probability of damage (SSPD)		
Cruise missile damage threshold		
Blue ACM inventory per ship		
Blue ACM service rate (per subinterval)		
Blue ACM SSPK		
Blue ABM inventory per ship		
Blue ABM service rate (per subinterval)		
Blue ABM SSPK		
CIWS SSPK		
Blue shooting policy		
Percentage of second shots (when shooting policy is not "shoot")		
Information quality		
Mean collaboration time		
Geometry overlap (COP case only)		
Future attack decision weight (COP case only)		

NOTE: As in the TCT case, design variables do not change and a range of values for each is plotted, provided it is quantitative. Rather than plotting the various MOEs against time, we plot against subintervals. All time-dependent variables (arrivals, service rates, etc.) are then converted to the subinterval scale. If the variable is categorical (such as shooting policy), changes are activated through various controls (slider bars, radio buttons, etc.).



RANDMR1449-5.8

Missile Defense (Blue Inputs)

Anti-BM inventory (per Aegis)	20
Aegis BM service rate (per t)	30
Anti-CM inventory (per Aegis)	40
Aegis CM service rate (per t)	30
Aegis anti-BM SSPK (pB)	0 78
Aegis anti-CM SSPK (pC)	0 80
CIWS SSPK (pZ)	0 85
Blue shooting policy	Shoot-Look-Shoot
Percent second shots	0 90
Information quality	1 00
Mean collaboration time	0 57
Geometry overlap	0 95
Future attack decision weight	0 00

Figure 5.8—Screen Shot of Blue Inputs

Measures of Effectiveness

The two MOEs used in this analysis are the mean number of ships surviving and the number of ballistic missile leakers. Each is described below.

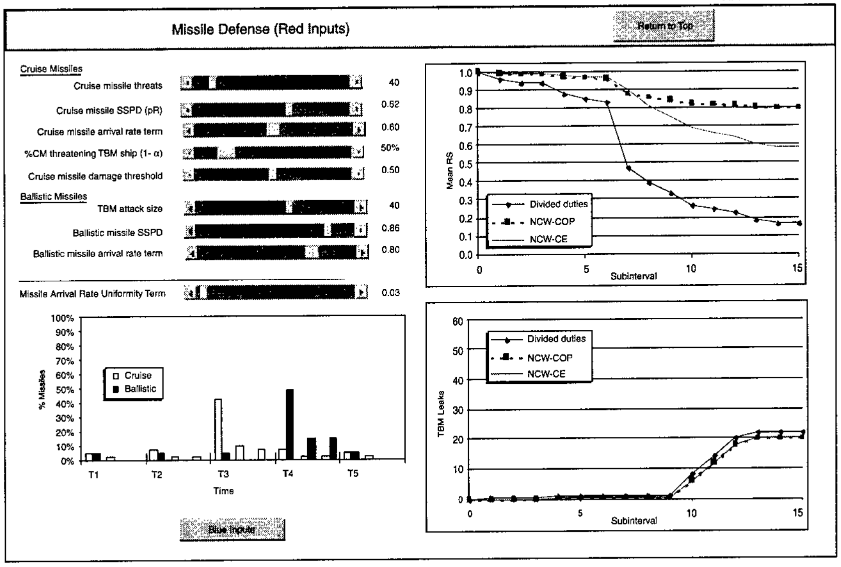
- **Mean Remaining Survival** in subinterval *j* is computed as

$$S_j = \frac{1}{2}\left[\left(1 - \frac{L_j^{(c)}}{N_L}\right) + \left(1 - \frac{L_j^{(b)}}{N_L}\right)\right],$$

  where N_L is the number of leakers required to destroy the ship and $L_j^{(i)}$ is the number of cruise missiles that have leaked through to ship *i* up to subinterval *j*.[5]

[5] See the discussion of the terminal defense queue in Chapter Three for a complete discussion of these terms.

RAND*MR1449-5.9*



Missile Defense (Red Inputs)

Cruise Missiles

Cruise missile threats 40

Cruise missile SSPD (pR) 0.62

Cruise missile arrival rate term 0.60

%CM threatening TBM ship (1- α) 50%

Cruise missile damage threshold 0.50

Ballistic Missiles

TBM attack size 40

Ballistic missile SSPD 0.86

Ballistic missile arrival rate term 0.80

Missile Arrival Rate Uniformity Term 0.03

Figure 5.9—Screen Shot of Red Inputs

- **Ballistic Missile Leaks** in subinterval *j* are computed as

$$B_j = \sum_{k=1}^{j} b_k \, ,$$

where B_j is the cumulative TBM leakers through subinterval *j*, and b_k is the number of TBM leakers in subinterval *k*.

Observations

The following are a few initial results that derive from examining the outputs:

- When the red cruise missile damage threshold is the same as the cruise missile single-shot probability of damage, then only one cruise missile is required to take an Aegis cruiser out of commission (OOC). This is a straightforward result from the calculation of the number of leakers required for OOC. That is, when $p_a = p_d$, we have that:

$$N_L = \frac{\ln(1-p_a)}{\ln(1-p_a)} = \frac{\ln(1-p_d)}{\ln(1-p_d)} = 1.$$

- When the missile arrival rate is equal across all intervals and subintervals, information quality has no impact on the decisions. This is because, in the absence of information, the default decision is based on a uniform arrival rate of enemy assets.

- If ACM inventories are not constraining so that both ships can attempt to intercept all incoming cruise missiles, the remaining survival MOE for the cooperative engagement case will be greater than or equal to the MOE for the shared COP case. This is because a higher kill probability is achieved when two ships are attempting to intercept incoming cruise missiles instead of one (unless the SSPK is 1 or 0). In the nonconstraining inventory example, the cooperative engagement decision will always be for all surviving ships to attempt cruise missile intercept, whereas in the shared COP case, both surviving ships will attempt to intercept only the cruise missiles in the geometric overlap. When the geometry overlap is one, the two cases will have equal values for the remaining survival MOE.

- There are instances when the remaining survival MOE is greater for the shared COP case than for the cooperative engagement case. This occurs because the objective of the cooperative engagement decision is to prolong the ability of at least one ship to perform the ACM role, not to minimize cruise missile leaks. In the cooperative engagement case, a large number of cruise missile leakers may be allowed, so long as the expected number of leakers realized by the end of the subinterval still allows the ship to function in an ACM role. Figure 5.8 illustrates an example of this where the two ships in the cooperative engagement case sustain more damage in the initial subinterval but whose cooperative planning allows them to last for two additional subintervals than in the COP case. The central authority in the cooperative engagement case decided to have only one ship defend against cruise missiles for the first six periods and then have both ships assume an ACM role.

- When ACM inventories are constraining and future expected cruise missile attacks are large, larger values of the future attack decision weight often lead to an early destruction of a ship. This is because a larger number of missiles arriving in the current period are left to be intercepted by the CIWS. Because the effective kill probability using only one friendly asset may be significantly smaller than using two, more leaks occur in the current period and the ship may be taken OOC earlier.

- For a fixed set of inputs, increasing or decreasing information quality often has little impact on altering the decision. This will occur when the projected distribution of arrivals in a subinterval is near uniform and the difference between the actual and projected is small. It will also occur when inventory levels are such that it is impossible to take advantage of the information. The computed expected missile arrivals in each subinterval is bounded by both the number of remaining missiles divided by the number of remaining subintervals and the actual number of arrivals. In many cases, decisions are the same for all values within that range, and so varying information quality has no impact on the action taken by the ships.

Chapter Six

CONCLUSION

We conclude this report as we began it: by emphasizing the need for new measures and metrics that incorporate the effectiveness of C4ISR systems, procedures, and equipment and their effect on combat outcome. The assertion is generally made that a richly connected network of C4ISR facilities and weapon systems will improve decisionmaking and therefore favorably impact combat operations. This may be true, but as yet we have no systematic, universally accepted way to demonstrate the truth of this claim. Consequently, analysis continues along two seemingly independent paths: one assessing the performance of C4ISR systems and one that focuses on the effects of weapon systems on combat outcomes. The longer analysts continue to employ only traditional MOEs in this bifurcated way, the longer they ignore the important effects of information and decisionmaking on combat outcomes. The services have recognized how important this is and have begun to sponsor important research in this area. This report has focused on the Navy's early attempts at codifying one approach. Clearly, much remains to be done before accepted practices can be established. The work presented here is just a beginning.

In this chapter, we conclude with a few first principles developed in the process of conducting this research. The focus is on methodology rather than results in that most of this work is theoretical and remains to be verified, validated, and calibrated. However, lessons can be learned from theoretical work, and we state these findings next.

REPRESENTING NETWORK-CENTRIC OPERATIONS

NCW is not just about networks. Networks are necessary but are not sufficient to achieve effective network-centric operations. Much has been made of the relationship between the "size" of the network and its efficiency. The computer network analogy is often cited to illustrate that a more richly connected network *ipso facto* improves overall performance. The claim is that performance improves with the square of the number of nodes in the network based on the work done in the 1970s by Robert Metcalf in assessing the effectiveness of the Hawaiian AlohaNet packet radio system for data communications. As compelling as this argument may be, it remains to be seen if this is true when applied to military operations.

A somewhat different claim is that the larger the number of connections in an operational network, the more likely individual nodes will experience "information overload." This is simply a paraphrased Parkinson's Law. That is, if a communication channel exists it is likely to be used. This too is compelling—however, like Metcalf's Law it remains to be seen if this is the case when applied to military operation.

We might think of these two claims as extremes in a network value measurement continuum. Truth is likely to be some combination of both expressed in, perhaps, a new metric.

Complexity

The issue centers on the effects of relying on a complex network to conduct military operations. What are the effects of complexity? Are there synergistic effects that can improve the efficiency of operations beyond Metcalf's n^2? Are there deleterious effects that reduce the efficiency on the order of, say, n^{-2}? More important, just what do these order-of-magnitude assessments mean when applied to combat operations? In this work, we suggested a way to assess both the good and bad effects of complexity with no claim that our representations are accurate. Clearly more needs to be done and we suggest further research in this area in our "Next Steps" section below.

However, complexity alone, as defined by the number of connections in a network, is clearly not enough to assess the effectiveness of network-centric operations. If it were, the obvious solution would be to return to platform-centric operations. The *command and control procedures* implemented on the network and the quality and extent of *collaboration* also play important roles, and we discuss them next.

Collaboration

Collaboration is expected to improve a process by which a team of individuals works together to achieve a common goal. Experimentation has verified that under some circumstances this is indeed true.[1] We have argued in this report that collaboration is important because it can enhance the degree of shared awareness in a group that is focused on solving a specific problem or arriving at an agreed decision. We have also suggested that although several reasons explain why collaboration might be expected to improve the degree of shared awareness, there may be ways in which it can degrade team performance. Capturing both effects in an MOP is problematic and should be the subject of further research.

Although, in this work, we have assumed that collaboration is generally beneficial, we have also recognized that it is not *uniformly* beneficial. The basic assumption means that as the opportunity for a decision team to collaborate increases (more connections), the better is the decision, whereas the variable benefit depends on the *quality* of the collaboration. Among the several factors that affect the quality of collaboration is the knowledge the team members possess about the critical element(s) of the operation. It is this important factor that we focus on in this research, and we appeal to information theory to assess its impact. We have purposely ignored other important effects on the quality of collaboration as well as collaboration that degrades performance. We suggest that this is also an area for future research.

[1] See Perry, Signori, and Boon (2001).

INFORMATION THEORY

Information theory is not just a subset of communications theory as some suggest.[2] Rather, it contributes to several fields of human endeavor, such as physics, computer science, statistical inference, philosophy, economics, and, for our purposes more importantly, military operations. In this work, we rely on information theory to assess the "amount" of knowledge available in a command and control system. To do this, we apply the important concept of information entropy or Shannon entropy. Where uncertainty exists, information entropy can be assessed—provided the uncertainty can be expressed as a probability distribution. The entropy measures the amount of information available in the distribution. We use this to make the intellectual leap to measuring the knowledge level about the uncertain random variable.

The quality of collaboration mentioned earlier is clearly related to the knowledge the participants in the decision team possess about the uncertain environment in which they operate. It is natural therefore to resort to the knowledge function, which is derivative of information entropy, to assess the effectiveness of the collaboration between two decision team members. As useful as this may be, we recognize that it remains to be seen (through analysis, experimentation, and simulations) just how true this is. In addition, we also recognize that the other elements of collaboration, those that fall more in the domain of human behavior, need to be included in the overall assessment. Experimentation, analysis, and simulations to verify our current hypothesis should also be the subject of future research.

EXPLORATORY ANALYSIS AND SPREADSHEET MODELS

Finally, we address the use of exploratory analysis as the first step in evaluating the effectiveness of the measures and metrics we have proposed. Exploratory analysis allows us to evaluate changes in MOEs that result from modifying the levels of input variables using visualization techniques. This allows us to better understand the structure of the data and the complex relationships that exist between the inputs and the MOEs. It is the first step because the tool,

[2] See Cover and Thomas (1991).

by its nature, omits much of the detailed nuances present in a high-resolution model.

The spreadsheet models developed to support this research are expected-value models and therefore lack the variational richness one might expect from stochastic simulations. The mathematical formulations, although apparently detailed, are really abstractions of the real world. This, coupled with the expected-value representation, lowers the level of resolution. This is more than compensated for by the ease with which the analyst is able to generate thousands of alternative solutions.

The exploratory analysis visualization techniques suggested in this report are by no means exhaustive. Any technique, visual or otherwise, that allows the analyst to sort the solutions quickly in some rational way is acceptable. Future research should focus on applying known visualization techniques and/or developing new ones. Another step in the process would be to build stochastic models that explore the variability inherent in the two vignettes.

NEXT STEPS

We have stated repeatedly that this report is but a small first step in the effort to establish measures and metrics to connect C4ISR and network-centric operations to combat outcomes. We have suggested areas requiring further research throughout the text, and we combine them here to emphasize their importance to achieving our goals:

- **Improve understanding of network complexity and better characterize its effects**: This is clearly a major undertaking. Our assessment in this work is essentially one-dimensional; complexity grows with the number of connections. Its effects are to both degrade and enhance performance. Although this sounds reasonable, much more of this subject needs to be understood and subsequently included in a comprehensive measure of performance.
- **Improve understanding of the effects of collaboration**: We have postulated that, like complexity, collaboration can have both good and bad effects. Sharing information will likely improve

shared awareness, and shared awareness will likely improve decisionmaking. However, what are the bad effects of collaboration and how can we capture them in an MOP?

- **Examine ways to represent the multidimensional effects of collaboration:** In the TCT example, collaboration was measured in terms of the knowledge each node had about the time required to complete a task. Clearly, other uncertainties exist that can be reduced through collaboration. Although these are likely to be situation-specific, the methodology used to combine them should be universal.
- **Assess the effects of information quality collaboration:** The quality of the information shared among the participants in the network will likely have a considerable effect on operations. How can we measure accuracy, completeness, and timeliness? What effect does this have on the quality of collaboration and how do we measure it?

Appendix

INFORMATION ENTROPY

The following is a detailed mathematical development of the information entropy function for the beta distribution used to represent the enemy missile arrival rate within each subinterval. Figure A.1 is a reproduction of Figure 3.10 in the main report.

THE BETA DISTRIBUTION

The beta probability density function is defined as follows:

$$f(x;\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1}, x\in[0,1],$$

with mean

$$E(x)=\frac{\alpha}{\alpha+\beta},$$

and variance

$$V(x)=\frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}.$$

For $\alpha=\beta=1$, the well-known uniform distribution results. For $\alpha,\beta>1$ the distribution has a mode:

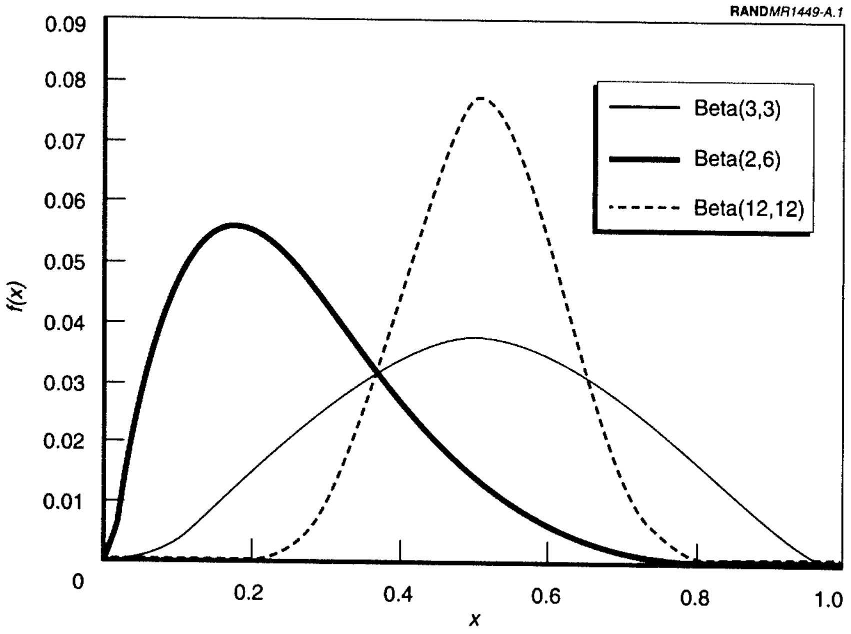


Figure A.1—The Beta Probability Density Function

$$\frac{\alpha-1}{\alpha+\beta-2}.$$

For this study, we consider only those distributions for which $\alpha,\beta \geq 1$. Figure A.1 illustrates the density for various values of α and β.

KNOWLEDGE CALCULATIONS

If we let $\hat{\lambda} = qx$ be the expected missile arrivals in the current subinterval, where q is the known inventory of remaining missiles, then x is a random variable. If we let $E(x) = \xi$, then the expected value of missile arrivals is $E(\hat{\lambda}) = qE(x) = q\xi$. Since ξ is the actual fraction of the remaining inventory scheduled to be launched in the current subinterval, we choose parameters of the beta distribution, α and β, such that $\alpha/(\alpha + \beta) = \xi$. However, because an infinite number of combinations of α and β can yield an unbiased estimate, we choose the appropriate values under the constraint that $\min(\alpha, \beta) \geq 1$ (ensuring that a mode exists) and such that the resulting variance achieves a target value $V_0(x)$. The *target variance* reflects the information quality, Q, associated with the sensor suite used to produce the estimate of missile arrival rate for the current period.

For purposes of this discussion, information quality is the degree to which the information is current, correct, and complete. Therefore, we set $0 \leq Q \leq 1$, where $Q = 1$ implies the information has maximum quality.[1]

Target Variance

We let the target variance, $V_0(x)$, be the largest attainable variance given our constraints. That is, $V_0(x)$ represents the maximum-uncertainty case. We can then develop a beta distribution with mean ξ and variance $V_0(x)$ and associate it with $Q = 0$ (a large variance implies low quality). We further let $V_1(x)$ be the minimum variance. $V_1(x)$ then is associated with $Q = 1$. We now choose a scalar, $k \geq 1$, so that $V_0(x) = kV_1(x)$. From this, we can derive the variance, $V_Q(x)$, for any level of information quality, Q, as follows:

$$\begin{aligned} V_Q(x) &= V_0(x) + Q\big(V_1(x) - V_0(x)\big) \\ &= V_0(x) + Q\left(\frac{V_0(x)}{k} - V_0(x)\right) \\ &= V_0(x)\left[1 + Q\left(\frac{1}{k} - 1\right)\right]. \end{aligned}$$

If $\alpha_0, \beta_0 \geq 1$ are the parameter values that yield the largest possible variance, $V_0(x)$ whose mean is

$$\frac{\alpha_0}{\alpha_0 + \beta_0} = \xi,$$

[1] For a more complete discussion of information quality, see Perry, Signori, and Boon (2001).

we can use the preceding result to find the parameters $\alpha_Q, \beta_Q \geq 1$ for all values of Q and the true enemy missile arrival proportion, ξ. Figure A.2 illustrates the linear relationship.

Theorems

Before proceeding, we develop some important theorems.

Theorem 1: *(a) If*

$$\rho = \frac{V_Q(x)}{V_0(x)} = \left[1 + Q\left(\frac{1}{k} - 1\right)\right]$$

represents the target reduction in variance achieved by a specified level of sensor information quality, Q, and (b) if the original beta distribution with variance, $V_0(x)$*, and mean,* ξ*, has parameters* α *and*

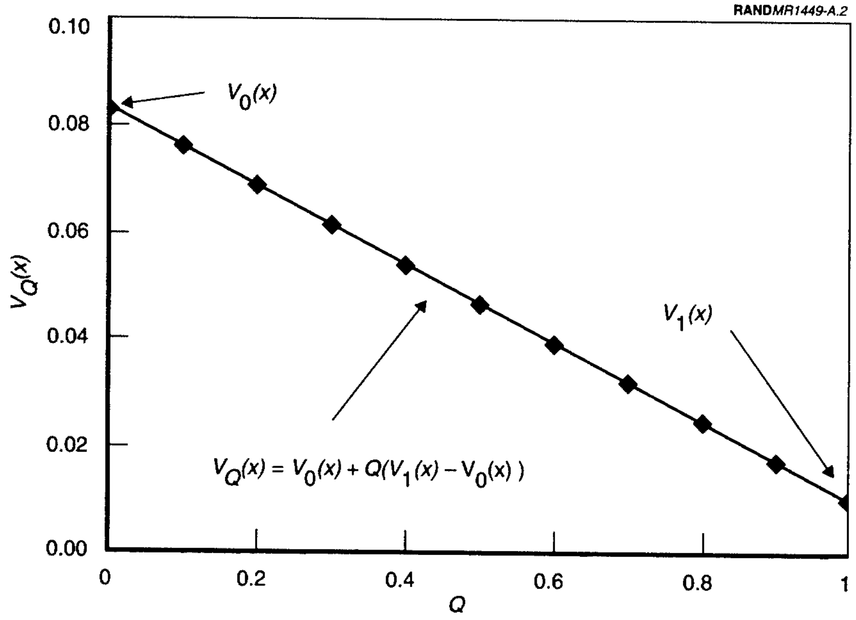


Figure A.2—Attack Distribution Variance from $V_0(x)$ and $V_1(x)$

β, *then the target beta distribution has parameters* $\alpha' = \delta\alpha$ *and* $\beta' = \delta\beta$, *where*

$$\delta = \frac{\frac{\alpha}{\xi} + 1 - \rho}{\rho\frac{\alpha}{\xi}}.$$

Proof: *Solving*

$$\frac{\alpha}{\alpha+\beta} = \xi$$

for β, *we get*

$$\beta = \alpha\frac{(1-\xi)}{\xi} .$$

Since

$$\rho = \frac{V_Q(x)}{V_0(x)},$$

for specified values of k and Q, we get the following:

$$\begin{aligned}\rho = \frac{V_Q(x)}{V_0(x)} &= \frac{\alpha'\beta'}{(\alpha'+\beta')^2(\alpha'+\beta'+1)} \bullet \frac{(\alpha+\beta)^2(\alpha+\beta+1)}{\alpha\beta}\\ &= \frac{\delta\alpha\delta\beta}{(\delta\alpha+\delta\beta)^2(\delta\alpha+\delta\beta+1)} \bullet \frac{(\alpha+\beta)^2(\alpha+\beta+1)}{\alpha\beta}\\ &= \frac{\delta^2\alpha\beta}{\delta^2(\alpha+\beta)^2(\delta\alpha+\delta\beta+1)} \bullet \frac{(\alpha+\beta)^2(\alpha+\beta+1)}{\alpha\beta}\\ &= \frac{\alpha+\beta+1}{\delta\alpha+\delta\beta+1}.\end{aligned}$$

Solving for δ *we get the desired result:*

$$\delta = \frac{\frac{\alpha}{\xi} + 1 - \rho}{\rho \frac{\alpha}{\xi}}.$$

Theorem 2: *Rescaling both parameters of a beta distribution by a constant,* $\delta > 1$, *will leave the expected value unchanged but will decrease the variance of the resulting distribution.*

Proof: *If the parameters are* $\alpha, \beta \geq 1$ *and we let parameters of the scaled distribution be* $\alpha' = \delta\alpha$ *and* $\beta' = \delta\beta$, *where* $\delta > 1$, *the expected value of the scaled distribution is:*

$$E(x{:}\alpha',\beta') = \frac{\alpha'}{\alpha'+\beta'} = \frac{\delta\alpha}{\delta\alpha+\delta\beta} = \frac{\delta\alpha}{\delta(\alpha+\beta)} = \frac{\alpha}{\alpha+\beta}.$$

For the variance, construct the ratio:

$$\begin{aligned}\frac{V(X;\alpha',\beta')}{V(X;\alpha,\beta)} &= \frac{\alpha'\beta'}{(\alpha'+\beta')^2(\alpha'+\beta'+1)} \bullet \frac{(\alpha+\beta)^2(\alpha+\beta+1)}{\alpha\beta} \\ &= \frac{\delta^2\alpha\beta}{\delta^2(\alpha+\beta)^2(\delta\alpha+\delta\beta+1)} \bullet \frac{(\alpha+\beta)^2(\alpha+\beta+1)}{\alpha\beta}. \\ &= \frac{\alpha+\beta+1}{\delta\alpha+\delta\beta+1} < 1 \text{ whenever } \delta > 1.\end{aligned}$$

From this we have that

$$\frac{V(x{:}\alpha',\beta')}{V(x{:}\alpha,\beta)} < 1$$

and therefore $V(x{:}\alpha', \beta') < V(x{:}\alpha, \beta)$.

Corollary 2a: *Rescaling both parameters of a beta distribution by a constant,* $\delta = 1$, *will leave the expected value and variance of the resulting distribution unchanged.*

***Proof:** If $\delta = 1$, then $\alpha' = \alpha$ and $\beta' = \beta$, so the distribution and its central moments are unaffected.*

***Corollary 2b:** Rescaling both parameters of a beta distribution by a constant, $\delta < 1$, will leave the expected value unchanged and increase the variance of the resulting distribution.*

***Proof:** Let $\alpha' = \delta\alpha$ and $\beta' = \delta\beta$, where $\delta < 1$. By theorem 2, the expected value of the scaled distribution remains unchanged. Also from the proof of theorem 2, we get:*

$$\frac{V(X;\alpha',\beta')}{V(X;\alpha,\beta)} = \frac{(\alpha+\beta+1)}{(\delta\alpha+\delta\beta+1)} > 1 \text{ whenever } \delta < 1.$$

Therefore $V(x{:}\,\alpha',\beta') > V(x{:}\,\alpha, \beta)$.

***Theorem 3:** For a beta distribution with parameters α', β' and mean $E(x) = \xi$ and with the condition that $\min(\alpha',\beta') \geq 1$, the largest attainable variance is achieved by setting $\alpha' = 1$ if $\xi \leq 0.5$ and setting $\beta' = 1$ if $\xi > 0.5$.*

***Proof:** From corollaries 2a and 2b, we maximize the variance by rescaling the parameters of a beta distribution with parameters $\alpha, \beta \geq 1$ by a constant $\delta \leq 1$. The constraint that $\min(\alpha', \beta') \geq 1$ implies that the largest constrained variance occurs when $\min(\alpha', \beta') = 1$. If*

$$\xi = \frac{\alpha'}{\alpha'+\beta'},$$

we must have that $\beta' < \alpha'$. This can occur only when $\beta' = 1$. Similarly, for

$$\xi = \frac{\alpha'}{\alpha'+\beta'} \leq 0.5,$$

we must have that $\beta' \geq \alpha'$. Consequently we must have $\alpha' = 1$.

Calculating Parameters for Maximum Uncertainty

We now use the theorems to calculate the parameters, $\alpha_0, \beta_0 \geq 1$, associated with the maximum uncertainty distribution. We first calculate the maximum variance, $V_0(x)$. We have that

$$\frac{\alpha_0}{\alpha_0 + \beta_0} = \xi .$$

Based on theorem 3, this can be accomplished by setting either $\alpha_0 = 1$ or $\beta_0 = 1$ depending on the value of ξ:

If $\xi \leq 0.5$ then set $\alpha_0 = 1$ and solve for

$$\beta_0 = \frac{1-\xi}{\xi} .$$

If $\xi > 0.5$ then set $\beta_0 = 1$ and solve for

$$\alpha_0 = \frac{\xi}{1-\xi} .$$

The target variance parameters are now calculated to be $\alpha_Q = \delta\alpha_0$ and $\beta_Q = \delta\beta_0$, for some $\delta > 1$ (resulting in a lower variance as shown in theorem 2). With this, we employ theorem 1 to solve for the new parameter values, α_Q and β_Q.

Entropy for the Beta Distribution

Entropy for the beta distribution with parameters α and β is calculated to be: [2]

[2] See Cover and Thomas (1991).

$$H(x) = -\int_{x=0}^{1} f(x)\ln f(x)dx$$
$$= \ln[B(\alpha,\beta)] - (\alpha-1)[\psi(\alpha) - \psi(\alpha+\beta)] - (\beta-1)[\psi(\beta) - \psi(\alpha+\beta)].$$

where $\psi(c)$ is the first derivative of Euler's gamma, and

$$B(p,q) = \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)}.$$

We can create a mapping of entropy onto a [0,1] knowledge scale by selecting an upper bound on the entropy associated with the fraction x. Before proceeding, however, we note that the uncertainty associated with the fraction of the remaining missiles arriving in the current subinterval is equivalent to the uncertainty associated with the actual arrival rate, λ, or $H(\lambda) = H(x)$.

The upper bound for $H(\lambda)$, denoted $H^*(\lambda)$, occurs when $\alpha = \beta = 1$. That is, maximum entropy occurs when uncertainty is maximized. In this case, therefore, we have that $H^*(\lambda) = 0$, a natural upper bound. A lower bound is also needed. However, minimum entropy occurs when the variance is minimized or when α and β are very large so that $H(\lambda) \to -\infty$. For practical purposes, we set this to be $\alpha = \beta = 12$, for which $H(\lambda) = -32.3192$. We can define knowledge therefore as:

$$K(\lambda) = 1 + \frac{H(\lambda) - H_{\min}(\lambda)}{H_{\min}(\lambda)} = \frac{H(\lambda)}{H_{\min}(\lambda)} = \frac{H(\lambda)}{-32.3192}.$$

Implementation

For the exploratory analysis tool discussed in Chapter Five, a value of $k = 8.333$ was selected for the equation $V_0(x) = kV_1(x)$. The value of k was determined to be the ratio of the variance of a beta(1,1) to a beta(12,12) distribution. Based on that, we also set $H^*(\lambda) = -32.3192$ which corresponds to the same symmetric beta(12,12) distribution.

Numerical Approximation of Euler's Gamma

The following code can compute an approximation to Euler's gamma accurate to 10 decimal places:

```
function psi($x$)
$x = x + 6$;
$p = 1/\mathrm{x}^2$;
$p = 0.004166666666667p^4 - 0.003968253986254p^3 +$
    $0.008333333333333p^2 - 0.83333333333333p$;
$p = p + \ln(x) - (0.5/x) - 1/(x-1) - 1/(x-2) - 1/(x-3) - 1/(x-4) -$
    $1/(x-5) - 1/(x-6)$;
$p = -p$;
return($p$);
end;
```

Successive calls to this function for $x = 1, 2, \dots, 12$ yield the results reported in Table A.1. These values were used in the exploratory analysis model described in Chapter Five.

Table A.1

Euler's Gamma

x	$\psi(x)$
1	0.5772156649
2	–0.4227843351
3	–0.9227843351
4	–1.2561176684
5	–1.5061176684
6	–1.7061176684
7	–1.8727843351
8	–2.0156414780
9	–2.1406414780
10	–2.2517525891
11	–2.3517525891
12	–2.4426616800
13	–2.5259950133
14	–2.6029180902
15	–2.6743466617
16	–2.7410133283
17	–2.8035133283
18	–2.8623368577
19	–2.9178924133
20	–2.9705239922
21	–3.0205239922
22	–3.0681430399
23	–3.1135975853
24	–3.1570758462
25	–3.1987425129
26	–3.2387425129
27	–3.2772040513
28	–3.3142410884

BIBLIOGRAPHY

This bibliography consists of documents and electronic media references that go beyond the scope of this report. The intent is to create a growing list of references to the topics this research is mainly concerned with, that is, MOEs, C4ISR, NCW and their application to Naval operations.

Alberts, S., J. Garstka, R. Hayes, and D. Signori, *Understanding Information Age Warfare,* Command and Control Research Program (CCRP) publication, 2001.

Alberts, D., J. Gartska, and F. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd ed., published by C4ISR Cooperative Research Program, 1999.

Annual Report on Military Power of People's Republic of China, U.S. Department of State —IIP: The United States and China, Report to Congress, 2000, www.usinfo.state.gov/regional/ea/uschina/dodrpt00.htm.

Ayyub, B., and R. McCuen, *Probability, Statistics, and Reliability for Engineers,* Boca Raton, Fla.: CRC Press, 1997.

Bankes, S., *Exploratory Modeling for Policy Analysis,* Santa Monica, Calif.: RAND, RP-211, 1993.

Blahut, R. E., *Principles and Practice of Information Theory,* Boston: Addison-Wesley, 1988.

Brooks, A., S. Bankes, and B. Bennett, *Weapon Mix and Exploratory Analysis: A Case Study,* Santa Monica, Calif.: RAND, DB-216/2-AF, 1997.

Cebrowski, A., and J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings,* Vol. 124, No. 1, January 1998, pp. 28–35.

Childs, J., *MOOTW and Information Superiority: The Importance of Continuity as a Principle of MOOTW in the 21st Century,* Naval War College Thesis, February 8, 2000.

Christian, R., *What Is Network Based Anti-Submarine Warfare?* http://spica.or.nps.navy.mil/netusw/WHITEPAPER.DOC.html.

Christofides, N., *Graph Theory: An Algorithmic Approach,* London: Academic Press, 1975.

Cover, T., and J. Thomas, *Elements of Information Theory,* New York: John Wiley & Sons, 1991.

Darilek, R., W. Perry, J. Bracken, J. Gordon, and B. Nichiporouk, *Measures of Effectiveness for the Information-Age Army,* Santa Monica, Calif.: RAND, MR-1155, 2001.

Davis, J., *Seventh Fleet to Conduct Fleet Battle Experiment Delta,* www.d7f.navy.mil/news/7frel266.html.

Davis, P., J. Bigelow, and J. McEver, *Exploratory Analysis and a Case History of Multiresolution, Multiperspective Modeling,* Santa Monica, Calif.: RAND, RP-925, 2001.

Fitzgerald, J. R., R. Christian, and R. Manke, "Network-Centric Anti-Submarine Warfare," *U.S. Naval Institute Proceedings,* Vol. 124, No. 9, September 1998, pp. 92–95.

FitzSimonds, J., "The Cultural Challenge of Information Technology," *Naval War College Review,* http://205.67.218.5/press/review/1998/summer/art1su98.htm.

Fleet Battle Experiment Alpha: Hunter Warrior, www.nwdc.navy.mil/mbchome/alpha/Default.htm.

Fleet Battle Experiment Bravo: Ring of Fire, Silent Fury, www.nwdc.navy.mil/mbchome/bravo/bravo.htm.

Fleet Battle Experiment Charlie: TAMD, AADC, www.nwdc.navy.mil/mbchome/charlie/charlie.htm.

Fleet Battle Experiment Delta: CSOF, Counter Fire, www.nwdc.navy.mil/mbchome/delta/fbe_d.htm.

Fleet Battle Experiment Echo: Asymmetric Urban Threat, www.nwdc.navy.mil/mbchome/echo/Default.htm.

Fleet Battle Experiment Foxtrot: Experiment Concept, www.nwdc.navy.mil/mbchome/foxtrot/Default.htm.

Fleet Battle Experiment Golf, www.nwdc.navy.mil/mbchome/golf/FBE_G.htm.

Garstka, J., "Network-Centric Warfare: An Overview of Emerging Theory," *Journal of the Military Operations Research Society,* December 2000, www.mors.org/Pubs/phalanx/dec00/feature.htm.

Gilder, George, "Metcalf's Law and Legacy," *Forbes ASAP,* September 13, 1993.

Hiniker, P., "The Common Operational Picture as Evolving Schema for Command Centers as Complex Adaptive Systems," *Proceedings of the 4th International Command and Control Research and Technology Symposium,* www.dodccrp.org/Proceedings/DOCS/wcd00000/wcd0006f.htm.

Holland, W., "Subs Slip Through the Net," *U.S. Naval Institute Proceedings,* Vol. 124, No. 6, June 1998, pp. 28–30.

Holzer, R., "Naval Air Defense Network Faces Key Test: U.S. Navy Admiral Raises Concerns About Readiness for Evaluation," *Defense News,* Vol. 3, No. 53, December 18, 2000.

Information Paper: Observations on the Emergence of Network-Centric Warfare, www.dtic.mil/jcs/j6/education/warfare.html.

Jackson, B., and D. Thoro, *Applied Combinatorics with Problem Solving,* Boston: Addison-Wesley, 1990.

Johnson, J., "Network-Centric Warfare: Real-Time Awareness," *All Hands,* January 1998.

Koopman, B., *Search and Screening: General Principles with Historical Applications,* New York: Pergamon Press, 1980.

Mitchell, R., "Naval Fire Support: Ring of Fire," *U.S. Naval Institute Proceedings,* Vol. 123, No. 11, November 1997, pp. 54–57.

Mullen, M., "Where Surface Warfare Is Headed and Why," *U.S. Naval Institute Proceedings,* Vol. 124, No. 10, October 1998, pp. 76–79.

Murray, T., *Experimenting with Fires: Toward a New Operational Concept,* Naval War College Thesis, May 17, 1999.

"Navy Theater-Wide Program: Taking Theater Ballistic Missile Defense to Sea," *Surface Warfare,* July/August 2000.

Nelson, J., S. Newett, J. Dworken, K. McGrady, and K. LaMon, *Measures of Effectiveness for Humanitarian Assistance Operations,* Alexandria, Va.: Center for Naval Analyses, Distribution Statement, April 1996.

Neter, J., and W. Wasserman, *Applied Linear Statistical Models,* Homewood, Ill.: R. D. Irwin, 1974.

Network-Centric Warfare, Naval War College Library Notes (bibliography), www.nwc.navy.mil/library/3Publications/Eccles%20 Library/LibNotes/libnetwork.htm, May 1999.

Network-Centric Warfare: Implications for Military Operations, www.dodccrp.org/NCW/imply_mil_ops.htm.

O'Hanlon, M., *Can China Conquer Taiwan?* Washington, D.C.: Brookings Institution, publication, July 2000.

Owens, W., "The Emerging U.S. System-of-Systems," *National Defense University Strategic Forum,* No, 63, February 1996, www.ndu.edu/inss/strforum/forum63.html.

Parkinson, C., *Parkinson's Law and Other Studies in Administration,* Boston: Houghton Mifflin, 1957.

Pecht, M., ed., *Product Reliability, Maintainability, and Supportability Handbook,* Boca Raton, Fla.: CRC Press, 1995.

Perry, W., and J. Moffat, "Measuring the Effects of Knowledge in Military Campaigns," *Journal of the Operational Research Society,* Vol. 48, No. 10, 1997, pp. 965–972.

Perry, W., D. Signori, and J. Boon, *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and Its Impact on Shared Awareness,* Santa Monica, Calif.: RAND, DRR-2389-OSD, 2001.

Report to the Congress: Pursuant to the FY99 Appropriations Bill, February 1, 1999.

Schultz, P., Capt., "Linebacker: Navy TBMD at Sea," *Surface Warfare,* January–February 2001, surfacewarfare.nswc.navy.mil/magazine/tbmdjanfeb.html.

Shannon, C., "A Mathematical Theory of Communication," *Bell System Technical Journal,* Vol. 27, 1948, pp. 379–423, 623–556.

Slais, T., Jr., *Some Principles of Network-Centric Warfare: A Look at How NCW Applies to the Principles of War,* Naval War College Thesis, February 5, 1999.

Stein, F., *Observations on the Emergence of Network-Centric Warfare,* Vienna, Va.: Evidence Based Research, Inc., publication, www.dodccrp.org/steinncw.htm.

Strategic Change, Transformation, and Military Innovation, Naval War College Library Notes (bibliography), Vol. 28, No. 5, March 2000, www.nwc.navy.mil/library/3Publications/Eccles%20Library/LibNotes/libstratinno.htm.

"Taiwan," *The World Factbook, 2000,* www.odci.gov/cia/publications/factbook/geos/tw.html.

"The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest,* Vol. 16, No. 4, 1995, pp. 377–396.

Wegner, D., "Transactive Memory: A Contemporary Analysis of the Group Mind," in Brian Mullen and George R. Goethals, eds., *Theo-*

ries of Group Behavior, New York: Springer-Verlag, 1987, pp. 185–208.

West, F., Jr., "Ring of Fire or Ring of Smoke?" *U.S. Naval Institute Proceedings,* Vol. 124, No. 11, November 1998, pp. 38–41.

"What Is Link-16," prodevweb.prodev.usna.edu/SeaNav/NS40x/NS401/Introduction/html/indexintro.html.

Winters, M., and B. Wilczynski, "Data Interoperability: Foundation of Information Superiority," *CHIPS,* July 2000.

In military operations, information has always been every bit as vital as fuel or ammunition in achieving favorable outcomes. Today, the need to reduce decision timelines highlights its importance. The Navy postulates that network-centric operations will enhance the effectiveness of combat systems by allowing commanders to mass effects from great distances. At issue is verification of this assumption. How can the effectiveness of network-centric information systems be linked to combat outcomes? The authors seek to identify how information affects outcomes and determine how to measure the link between the two. This report creates a framework for developing measures to help the Navy decide how network-centric operations affect combat outcomes and which information systems work best. The authors demonstrate a proof-of-concept tool that can generate several alternative network-centric command, control, communications, computer, intelligence, surveillance, and reconnaissance systems. Using a spreadsheet model, they take the first steps toward developing formulas to help the Navy codify an approach to measuring combat effectiveness in network-centric operations.

ISBN 0-8330-3139-2

52400

9 780833 031396